

# 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.

© 2019 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](http://www.NEXUSInstitute.net)



[@NEXUSInstitute](https://twitter.com/NEXUSInstitute)

All rights reserved. This publication may be reproduced in whole or in part and in any form for educational or non-profit purposes without special permission from the publisher, provided acknowledgement of the source is made. Email: [Office@NEXUSInstitute.net](mailto:Office@NEXUSInstitute.net)

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](http://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](http://www.WarnathGroup.com).




**Stephen Charles Warnath**  
**Founder, President & CEO**  
**NEXUS Institute**

# Table of Contents

<b>FOREWORD</b> .....	<b>2</b>
<b>TABLE OF CONTENTS</b> .....	<b>6</b>
<b>ACRONYMS AND ABBREVIATIONS</b> .....	<b>9</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>11</b>
<b>1. INTRODUCTION</b> .....	<b>35</b>
<b>2. RESEARCH METHODOLOGY</b> .....	<b>37</b>
 2.1 DESK RESEARCH – LITERATURE AND DOCUMENT REVIEW .....	37
 2.2 INTERVIEWS WITH KEY INFORMANTS .....	37
 2.3 REVIEW PROCESS .....	40
<b>3. WHAT IS TIP DATA AND TIP DATA COLLECTION?</b> .....	<b>41</b>
Data collected for administrative purposes .....	42
Data collected for research purposes .....	43
Distinguishing between data used for administrative purposes and research purposes.....	43
Emerging types of TIP data .....	43
<b>4. LEGAL AND ETHICAL CONSIDERATIONS IN TIP DATA COLLECTION</b> .....	<b>45</b>
 4.1 DETERMINING APPLICABLE LAW AND RELEVANT ETHICAL ISSUES .....	45
 4.2 INTERSECTIONS BETWEEN LAW AND ETHICS IN TIP DATA COLLECTION.....	66
<b>5. LEGAL FRAMEWORKS IN TIP DATA COLLECTION</b> .....	<b>71</b>
 5.1 IDENTIFYING RELEVANT LEGAL FRAMEWORKS FOR TIP DATA COLLECTION.....	72
 5.2 NATIONAL LEGAL FRAMEWORKS .....	76
Scope and applicability.....	78
Definitions .....	79
Rights and obligations (or guiding principles) .....	79
Regulating bodies and compliance.....	80
 5.3 REGIONAL LEGAL FRAMEWORKS .....	81

European Union.....	82
Africa.....	88
Asia-Pacific .....	91
Organization of American States.....	94
 5.4 INTERNATIONAL LAW .....	95
 5.5 GUIDELINES, MANUALS AND PROCEDURES .....	97
 5.6 SUMMARY.....	99
<b>6. ETHICAL FRAMEWORKS IN TIP DATA COLLECTION .....</b>	<b>101</b>
 6.1 ETHICS REVIEW .....	105
 6.2 RESEARCH AND DATA COLLECTION PARTNERSHIPS.....	109
 6.3 SELF-ADMINISTERED ETHICAL STANDARDS AND GUIDELINES .....	111
 6.4 PEER REVIEW PROCESSES .....	117
 6.5 INFORMAL THIRD-PARTY ENGAGEMENT IN PROTECTION.....	118
 6.6 SUMMARY.....	120
<b>7. EMERGING ISSUES IN TIP DATA COLLECTION.....</b>	<b>122</b>
 7.1 INFORMATION COMMUNICATIONS TECHNOLOGY AND THIRD-PARTY TECHNOLOGY PROVIDERS .....	123
7.1.1 Data ownership in the context of ICT .....	123
7.1.2 Data sharing with third-party technology providers .....	124
7.1.3 Reliance on third-party technology providers .....	127
7.1.4 Anti-trafficking responsibilities of ICT providers.....	130
 7.2 USING BIG DATA IN ANTI-TRAFFICKING WORK .....	131



7.2.1 Risks posed by Big Data.....	132
7.2.2 The need for oversight of Big Data.....	136
 7.3 USING OPEN DATA IN ANTI-TRAFFICKING WORK .....	138
7.3.1 Opportunities of Open Data .....	139
7.3.2 Risks and issues with Open Data .....	141
 7.4 PRIVATE SECTOR ENGAGEMENT IN ANTI-TRAFFICKING .....	143
7.4.1 Supply chain accountability.....	144
7.4.2 Public-private partnerships .....	148
7.4.3 Defamation and other risks of collecting private sector data.....	150
 7.5 SUMMARY .....	151
<b>8. CONCLUSION .....</b>	<b>153</b>
<b>9. BIBLIOGRAPHY .....</b>	<b>156</b>

## 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 necessarily 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.



## 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, both for data subjects and for data collectors. It has been acknowledged that:

...addressing [trafficking in human beings] is an area that requires significant processing of data, in many cases involving personal data and consequently also creates risks of intrusions into privacy. Therefore, an effective action to address [trafficking in human beings] (THB) cannot be put in place without the support of a solid data protection scheme complementing it.<sup>1</sup>

At the same time, there remain substantial gaps in data available to inform anti-trafficking efforts. Moreover, there are many legal and ethical complexities at play in how researchers and anti-trafficking 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 ethical and legal 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 ethical and/or legal framework and so on. With increased emphasis on gathering TIP data and emerging technologies across all forms of data collection, there is a growing need to better understand, formulate and implement a framework for practice and operational standards across non-governmental organizations (NGOs), governments, technology companies and users of data, whether industry information service providers, policy units or law enforcement.

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. We examine legal and ethical issues in the context of traditional types of data collection (data collected for research and administrative purposes) as well as new forms of and approaches to TIP data collection, including the use of Big Data and Open Data as well as data collected in the context of private sector engagement, supply chain work and through information communications technology (ICT)/third-party technology providers. There is a range of issues related to data collection that are emerging alongside of and, to some extent, as a result of an increasingly diverse group of stakeholders becoming involved in anti-trafficking work, which often involves TIP data collection. 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

---

<sup>1</sup> EDPS (2012) *Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – ‘The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016’*. Brussels, Belgium: European Data Protection Supervisor, p. 2.

unresolved. This exploration also, by extension, has the goal of identifying 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. It is a contribution to emerging and important discussions of how to move forward with legal and ethical TIP data collection in an evolving and expanding terrain. The intention is to encourage careful consideration of these complicated issues, while acknowledging the complexity and grey zones in how TIP data is and should be collected and protected. We do not attempt to be authoritative or prescriptive, but rather to contribute to thinking on the issues that the anti-trafficking field is now grappling with in terms of TIP data collection. We consider this to be an opportune time for TIP data collectors – and funders of TIP data collection and research – to engage in reflection and discussion in order to move forward in the best possible way to ethically and legally collect the information that is needed to prevent and combat trafficking in persons globally.

After laying out the background and methodology for this study in Section 2, we outline and define, in Section 3, what constitutes TIP data collection. Recognizing that different TIP data collectors and different forms of data collection will elicit different ethical issues and applicable laws, in Section 4, we discuss the determination of applicable law and relevant ethical issues, including the categories of data collection that require specific consideration. We then consider intersections between law and ethics in TIP data collection, noting that a useful overlap between what is legal and what is ethical can be found in the underlying principles that inform the frameworks for both. Section 5 discusses legal frameworks for TIP data collection at the national, regional and international levels. Section 6 then explores ethical frameworks for TIP data collection. Finally, in Section 7, we consider the adaptation of existing legal and ethical frameworks to the emerging issues in TIP data collection, including related to ICT and third-party technology providers; Big Data; Open Data; and private sector engagement in anti-trafficking.

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 aimed to identify and mobilize 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). Other papers in the series include: *The Science (and Art) of Understanding Trafficking in Persons: Good Practice in TIP Data Collection*; *On the Frontlines: Operationalizing Good Practice in TIP Data Collection*; and *Good Practice in TIP Data Collection: Recommendations for Donors and Funders*.



## 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

NEXUS conducted 163 interviews with 128 key informants representing non-governmental organizations (NGOs), research projects, academic institutions, international organizations (IOs), private sector actors and government.<sup>2</sup> We identified key informants through our desk research and based on our selection criteria. While criteria differed somewhat by category of respondent, a central aspect was diversity with regard to: 1) the types of TIP data being collected (for example, on protection or prosecution); 2) the approaches and methods used; 3) geographic scope; and 4) professional specialty or discipline. We then conducted snowball sampling, contacting key informants recommended by those already interviewed and who met our selection criteria.

---

<sup>2</sup> We conducted follow-up interviews with select key informants as further questions arose during desk research or in the context of other interviews. This afforded not only greater depth to the information gathered, but also the opportunity to test and corroborate certain perspectives, assessments or findings.

**Interviews with TIP researchers and TIP experts.** We conducted 95 interviews with TIP researchers and TIP experts (67 first interviews and 28 follow-up interviews). This included TIP research experts (that is, researchers from different disciplines who are specialized in research on trafficking in persons), TIP experts who have experience in TIP data collection in their professional capacities (for example, as prosecutors, police, social workers or medical personnel) and TIP researchers from other professional fields (for example, individuals researching or collecting data on labor, migration and human rights, public health or child protection), as well as private sector actors engaged in anti-trafficking data collection. Lines of inquiry included: what constitutes protection and prosecution data; criteria or characteristics of good (and bad) practice in TIP data collection; gaps in TIP knowledge; key challenges in undertaking TIP data collection; and legal issues and ethical considerations in TIP data collection.

**Interviews with TIP data collection staff.** We conducted 55 interviews with individuals working on TIP data collection projects (49 first interviews and six follow-up interviews).<sup>3</sup> These were individuals working on TIP data collection projects (largely within NGOs, the United Nations (UN) and IOs, but also some government partnerships), donors funding TIP data collection projects and technology experts whose work encompasses TIP data collection. Data collection projects were initially identified through desk review, which included not only a review of research and resources but also searching the websites of organizations or institutions with TIP data collection projects. We also identified projects and key informants from different countries and regions based on recommendations from TIP research and experts interviewed for the project. Lines of inquiry included: details of the specific data collection project; challenges and lessons learned across the five stages of data collection; various considerations in undertaking TIP data collection; and legal issues and ethical considerations in TIP data collection.

**Interviews with National Rapporteurs or equivalent mechanisms.** We conducted 13 interviews with twelve staff from ten National Rapporteur offices or equivalent mechanisms from various countries in Europe and the Middle East.<sup>4</sup> In addition, we communicated with one National Rapporteur office in Europe by email and attended a presentation by one equivalent mechanism in Southeast Asia. We also reviewed research and data collection undertaken by National Rapporteurs or equivalent mechanisms as well as different models in Europe, the Caribbean, Latin America and Southeast Asia. Interviews focused on: the specific work and mandate of the National Rapporteur or equivalent mechanism; how specific data collection efforts were undertaken; challenges and lessons learned across the five stages of data collection; contextual considerations in the specific country in which the National Rapporteur or equivalent mechanism works; and any legal or ethical issues identified.

---

<sup>3</sup> There is some overlap between the categories of TIP researchers and TIP experts, on the one hand, and TIP data collection staff, on the other, as many professionals have worked in multiple roles. For the purpose of this categorization, TIP data collection staff are those whose interviews focused on their work on a specific data collection effort.

<sup>4</sup> A National Rapporteur is responsible for monitoring and reporting on the implementation of anti-trafficking policy at the national level and coordinating a country's anti-trafficking efforts. Some countries do not have an established National Rapporteur but use an alternative mechanism ("equivalent mechanism") for monitoring and reporting. A National Rapporteur or equivalent mechanism is "instrumental in aiding participating States to produce, analyze, utilize and report on quantitative and qualitative data needed to improve counter-trafficking actions". Warnath, S. (2008) *Efforts to Combat Trafficking in Human Beings in the OSCE Area: Co-Ordination and Reporting Mechanisms*. Vienna, Austria: Organization for Security and Co-Operation in Europe, p. 72. See also CoE (2009) *Council Conclusions on Establishing an Informal EU Network of National Rapporteurs or Equivalent Mechanisms on Trafficking in Human Beings*. Strasbourg, France: Council of Europe; and European Commission (2018) 'National Rapporteurs and/or Equivalent Mechanisms', *Together Against Trafficking in Human Beings*. Brussels, Belgium: European Commission.

*Table #1. Interviews conducted with TIP researchers and TIP experts, TIP data collection staff and National Rapporteurs or equivalent mechanisms*

<b>Type of key informant</b>	<b>Number of interviews</b>
TIP researchers and TIP experts	95
TIP data collection staff	55
National Rapporteurs or equivalent mechanisms	13
<b>Total</b>	<b>163</b>

All 163 interviews were conducted using standardized research instruments. Interviews were conducted in English with the exception of one interview with a National Rapporteur where the researcher was fluent in the language used. Researchers adapted lines of inquiry according to the specifics of the individual’s experiences, but standardized probes assisted researchers in maintaining commonality and consistency. In some instances, we conducted follow-up interviews with certain key informants as questions and issues arose over the course of the project, during desk research or in the context of other interviews.<sup>5</sup> Each interview began with a process of informed consent, which included an explanation of the purpose of the research, what the interview would involve, an overview of the questions that would be asked, how the data would be used/presented, the key informant’s right to decline to answer any questions or end the interview at any time and assurances of anonymity. Once explained, if the key informant consented, the researcher commenced the interview. Interviews were either in person or remote (via Skype or telephone) and were audio recorded, with the consent of the key informant. Interviews were typically 75-90 minutes in length. Once completed, the interviews were transcribed verbatim. All interviews were treated confidentially; transcripts were shared only within the research team and secured according to NEXUS Institute’s data protection policies. Information shared in this publication has been anonymized.

The geographic focus of key informants’ work covered most regions of the world, as shown on the map below. Some regions were more represented than others, a bias which we offset through the literature review and desk research

---

<sup>5</sup> We conducted 35 follow-up interviews (23 individuals were interviewed twice and seven individuals were interviewed three or more times).



Map #1. Geographic representation of research and data collection by key informants<sup>6</sup>



### 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.

<sup>6</sup> Most key informants work or conduct research in more than one country or even region, accounting for the discrepancy between the 128 respondents interviewed and the representation by region on this map.



### 3. What is TIP Data and TIP Data Collection?

Data collection is a broad concept, referring to a wide range of practices related to the process of gathering and measuring information on variables of interest. Data collection includes research conducted by researchers, institutions or organizations, as well as a broad assortment of administrative data collection by various organizations and institutions. Robust data collection is essential in maintaining the integrity of any analysis or data use. When data collection is conducted properly and ethically it allows data collectors and analysts to: effectively analyze and use data and findings; contribute understanding and knowledge to the TIP field; and inform effective policies and programs to address human trafficking. Improperly or unethically collected data may result in:

#### UN definition of trafficking in persons

The recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.

- an inability to answer data collection questions accurately;
- distorted or inaccurate findings and misleading conclusions;
- an inability to repeat or validate the process of data collection;
- harm to data collection participants;
- the potential to compromise interventions designed with the data;
- insufficient data to meet the research objectives.<sup>7</sup>

TIP data<sup>8</sup> is qualitative or quantitative information on trafficking in persons. Pieces of data are essentially individual pieces of information. Data is collected, managed and stored and then analyzed, after which it is used (for example, presented in written form or visualized using graphs, images or other analysis tools). For the purposes of this publication, TIP data collection is the overarching process of gathering and assigning meaning to data on various aspects of trafficking in persons, including its scope and nature and also anti-trafficking responses. This involves not only data collection itself but the processing and management of the data as well its analysis, use, presentation and dissemination.<sup>9</sup>

<sup>7</sup> ORI (2005) 'Data Collection', *Responsible Conduct in Data Management*. United States: Office of Research Integrity.

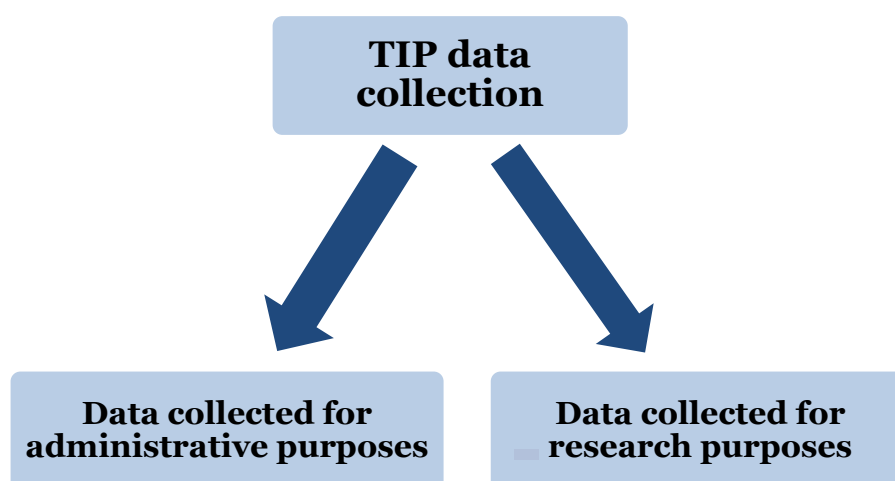
<sup>8</sup> This study largely treats the word "data" as an uncountable or collective noun rather than a plural, its Latin origin notwithstanding. By extension, we refer to "a piece of data" rather than "a datum" where called for. This is in line with established use and with leading style references for both UK and U.S. English. In some cases, the plural may nonetheless be applicable (for example, when referring to a grouping of several types of data).

<sup>9</sup> For the purpose of this study we have divided the TIP data collection process into five constituent parts as follows: 1) design and planning, 2) data collection, 3) data storage, maintenance and management, 4) data analysis and 5) use, presentation and dissemination. Each stage is explained and discussed in subsequent sections. When referring to TIP data collection we are referring to all of these five stages.

TIP data collection varies substantially in scope and nature. It may be undertaken by governments, IOs, NGOs, businesses and private sector actors. It may be global in scope and collated in a large and technically complex database. It may also relate to very specific and targeted data collected by a single organization or person to answer a very specific question. In some cases, it may constitute a discrete research project. In other cases, it may be the collection of administrative and research data as part of TIP-specific data collection efforts (for example, by the offices of National Rapporteurs or equivalent mechanisms). In still other cases, it may be administrative data collected as part of a project or an institution's ongoing operational work, either specific to TIP or more generally, such as social services or law enforcement. It also includes the collection of data to monitor or evaluate anti-trafficking interventions.

In discussing TIP data collection for the purpose of this study, we are primarily concerned with what we consider two distinct categories of TIP data: 1) Data collected for administrative purposes and 2) Data collected for research purposes.

*Diagram #1. Different types of TIP data collection*



### ***Data collected for administrative purposes***

This refers to information collected primarily for administrative purposes. This type of data is collected by government departments as well as NGOs and IOs for the purposes of registration, transaction and record keeping in the context of operational work with trafficking victims, usually during service delivery (for example, healthcare, social work, or legal assistance).<sup>10</sup> This includes, for example, case files about trafficking victims being assisted by an NGO or government office. Administrative data also includes that which comes from operational work in the legal process (for example, investigative files, court files and outcomes, data collected about perpetrators of crime and their cases within the criminal justice system). Sources of administrative data include the agencies, authorities and services that engage with victims or perpetrators of trafficking and violence (for example, police, prosecutors, judiciary, immigration officials, health services, social services and specialized service providers, both government and NGO). Some administrative data is specifically about TIP (for example, case files about trafficking victims being assisted by a dedicated NGO or from criminal justice records about TIP cases). In other cases, TIP administrative data is embedded within wider systems of data collection (for example, TIP cases within a broader criminal justice database, TIP cases among vulnerable persons assisted by state social services, or TIP as one form of human rights violations).

<sup>10</sup> ADLS (2017) 'Administrative data introduction', *Guidance to apply for and use administrative data*. United Kingdom: Administrative Data Liaison Service.

### ***Data collected for research purposes***

Here we refer to deliberate and discrete data collection on a specific issue in order to answer a specific question or address a specific hypothesis.<sup>11</sup> Research data may be collected by researchers, governments, NGOs, IOs and private sector actors and may be collected by a range of methods (for example, through interviews, questionnaires, focus group discussions, or surveys) whether in person or remotely (for example, by telephone or online). Research data may include primary and/or secondary data.<sup>12</sup> Some research is TIP-specific, while other research considers TIP within wider issues of migration, labor issues, vulnerable groups and so on.

### ***Distinguishing between data used for administrative purposes and research purposes***

We find it helpful to distinguish between data collected for administrative purposes and data collected for research purposes. These two types of data collection have different intentions and, by extension, also different approaches and procedures. Whereas the former is collected in the context of operational work (for example, service delivery to victims or the criminal justice process), the latter is collected specifically for research purposes.

This is not to say that administrative data cannot be used for research purposes. Indeed, it is an important data source for much TIP research.<sup>13</sup> However, because administrative data is collected as part of operational work, its primary purpose is practical and operational. This means that, in practice, administrative data is not always collected in a sufficiently rigorous way as to be helpful or appropriate for some research and data collection efforts. Generally speaking, when collecting and analyzing administrative data for research purposes, the same stringent standards should apply as when collecting research data. Questions, therefore, arise as to when administrative data can be used for research (and for what types of research) and what limitations need to be understood from the outset.

### ***Emerging types of TIP data***

TIP data collection is an emerging and evolving area of work, with an ever-expanding group of people working to collect TIP data. It may involve a range of actors, including governments, non-governmental organizations (NGOs), international organizations (IOs), academics, independent researchers and private companies. Some actors may not be involved in anti-trafficking work, but nonetheless may be engaged in TIP data collection, such as private companies that collect proprietary supply chain information or individuals or organizations who are contracted to collect certain information when TIP data collection is outsourced.

TIP data collection may also increasingly include less traditional types of data, including data from supply chains,<sup>14</sup> Open Data<sup>15</sup> and Big Data.<sup>16</sup> For example, private sector actors collect

---

<sup>11</sup> Walby, S. et al. (2017) *The concept of measurement of violence against women and men*. Bristol, United Kingdom: Policy Press.

<sup>12</sup> Primary data is data collected directly by the researcher or data collector (for example, through interviews, participant observation, life histories, case studies, questionnaires, surveys, ethnographic research and so on). Secondary data is that which has already been collected and can be used for analysis (for example, previous research, official statistics, archival materials such as diaries and letters, government reports, victim case files, court document, or police files).

<sup>13</sup> A data source is the source of the information being collected. A data source may consist of individuals (for example, trafficking victims, traffickers or perpetrators, service providers, or criminal justice representatives), as well as written materials (for example, register data, literature, or any other datasets).

<sup>14</sup> A supply chain is the system of organizations, individuals, activities and resources involved in in the production and distribution of a commodity. Kenton, W. (2017) 'Supply Chain', *Markets & Economy*, November 2017.

<sup>15</sup> "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. Sheriff, M. (2010) 'What "open data" means - and what it doesn't', *opensource.com*, December 10.

<sup>16</sup> "Big Data" is defined by the UN as "extremely large datasets associated with new information technology and which can be analyzed computationally to reveal possible patterns, trends and correlations". OHCHR (2016) *A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance*

Big Data that is essentially collected for commercial (market research) purposes but is increasingly being considered in terms of relevance to TIP and other forms of exploitation. Similarly, some administrative data (for example, case management data about assisted trafficking victims) may be being converted to Open Data, to be made available for researchers and analysts. And as private sector engagement is now considered an integral part of the anti-trafficking response, there is substantial data being collected on company supply chains. This means that, in some contexts, these new and different types of data need to be increasingly integrated into how we define TIP data collection as well as how these relate to legal and ethical considerations and requirements. 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. These issues are discussed in the following sections.

---

*Note to Data Collection and Disaggregation.* Geneva, Switzerland: Office of the United Nations High Commissioner for Human Rights, p. 12 at fn 25.



## 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. Responsible data has been defined as referring to the “duty to ensure people’s rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness.”<sup>17</sup> 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. All relevant stakeholders should be fully informed about and comprehend measures needed to adhere to legal and ethical frameworks, particularly those in a position to implement what are often complex and, sometimes costly, data protection measures.

In some countries and across some regions, legal and ethical frameworks surrounding TIP data collection (and 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 able to 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. Where data collection takes place in the context of administrative data collection (for instance, in the medical sphere), the legal framework is often clear. However, where data is collected in other contexts, such as via a survey as part of a wider research project, it may be less clear which legal framework, if any, applies.

It is also necessary to take into account and tackle issues that arise in the context of emerging types of data collection and the increased use of technology, including around information communications technology (ICT),<sup>18</sup> the collection and use of Big Data and Open Data and

---

<sup>17</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment*. Responsible Data Forum, p. 16.

<sup>18</sup> Information communications technology (ICT) refers to technologies that provide access to information through telecommunications. ICT includes the internet, wireless networks, cell phones and other communication mediums. Tech Terms (2017) ‘ICT Definition’, *Tech Terms*.

private sector engagement. These all raise issues related to data ownership and use involving multiple stakeholders and across many jurisdictions. In an era of electronic data collection and increasing technological solutions, data can be collected, stored and shared globally, resulting in multifaceted considerations for both ethics and law. For example, an NGO is subject to the laws and regulations of the country in which it is established but may be carrying out data collection in another country that applies different laws and regulations. When the entity providing funding for the data collection is from another country this may introduce further laws and regulations. Moreover, data may be stored in yet another country or “in the cloud”,<sup>19</sup> which is inherently global and subject to various and rapidly-changing national and international laws.<sup>20</sup> In some cases, applicable national laws or standards may conflict with or contradict international laws or standards.

Different types of data collection will involve different legal and ethical considerations. 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 in persons (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 with regard to legal and ethical issues depending on the type of data being collected and from whom. 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, notably data collected about trafficking victims; data collection involving suspects and/or convicted criminals, including human traffickers; and data collection with anti-trafficking professionals and stakeholders.

#### Categories of data collection that require specific consideration

- Data collection involving vulnerable persons, including children and trafficking victims
- Data collection that includes personal and/or sensitive data, notably data collected about trafficking victims
- Data collection involving suspected or convicted criminals, including human traffickers
- Data collection with anti-trafficking professionals and stakeholders

Again, there are distinctions to be made between legal and ethical considerations in TIP data collection. While the particular categories of data discussed below will have legal implications that a data collector *must* respond to in order to comply with 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 section is to encourage the development of an ethical framework to accompany and strengthen the implementation of the relevant legal framework for data collection. The development, further articulation and implementation of both legal and ethical frameworks are needed to ensure the collection of responsible data on trafficking in persons.

A key factor underpinning the development of ethics and laws on data collection is the risk of harm posed to **data collection subjects (human subjects)**.<sup>21</sup> Such harm may be acute in

<sup>19</sup> The cloud refers to software and services that run on a server or a network of servers. In simple terms, cloud computing means “storing and accessing data and programs over the internet instead of your computer’s hard drive”. Griffith, E. (2016) ‘What is Cloud Computing?’, *PC Magazine*, May 3.

<sup>20</sup> Andrews, D.C. and J.M. Newman (2012) ‘Personal Jurisdiction and Choice of Law in the Cloud’, *Maryland Law Review*, 73(1). See also Elkhatib, Y. (2015) ‘Explainer: where is “the cloud” ...and who owns it?’, *The Conversation*, December 8.

<sup>21</sup> A human subject is defined as a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information. See United States (2009) *Code of Federal Regulations*, Title 45, Part 46, Section 46.102. The

trafficking contexts (for instance, a person collecting administrative data may be required to breach confidentiality in some situations). As an example, in some countries laws require health care professionals to report either to law enforcement or child protection agencies as a result of an interaction with a victim of human trafficking (for example, mandatory child abuse reporting laws, domestic violence reporting laws, and laws requiring reports of knife or gunshot wounds).<sup>22</sup> This means that a medical practitioner collecting administrative data in these contexts must reconcile a legal obligation to report information about the individual to authorities with the ethical duty to maintain a patient's confidentiality. One way to try to balance these ethical and legal tensions is to ensure that data subjects are fully informed of any legal obligation on the part of the data collector to report to law enforcement. As one researcher explained:

With anyone, but especially with trafficking victims, they've been betrayed and manipulated and defrauded so much that it would be a terrible thing for a healthcare provider to do the same thing by not being clear about why they're asking questions or what they're going to do with the information. And especially if they... got this very confidential information, turned around and said, "Well, I'm going to go call police now because I have to". I think that would... just be reinforcing the victim's sense of helplessness and being betrayed. So, I think being right up front, start by saying: "There's a chance I might have to tell somebody about this so you can decide how much you want to tell me" is fair to them and it conveys respect.

Similarly, situations may arise where the person collecting data becomes aware that a person is being harmed by third-parties, whether in a trafficking or other situation. In such situations, while there may be no legal obligation to report to authorities, there could be an ethical obligation to do so, even when doing so is tantamount to breaching confidentiality. What constitutes the right or wrong action in a given situation will depend on legal requirements, ethical considerations and a case-by-case assessment of risks by the person in the position of having to make such decisions.

Indeed, researchers have expressed concern about universal declarations and *a priori* determinations<sup>23</sup> about what constitutes and will cause harm *versus* a case-by-case assessment. Such universal declarations are often made by identifying particular categories of persons who are vulnerable or by implying that by gaining informed consent, harm may somehow be mitigated. One set of ethical guidelines elaborates:

We agree that in certain extreme situations, there will be broad consensus about whether certain actions are ethical or not. Yet we also agree as a community of researchers that in most social situations, the issues and ethics are more fuzzy. It can be difficult if not impossible to predict beforehand what might cause immediate or eventual harm, whether or not someone is vulnerable, or even whether or not we can call something a "human subject". Hence the need for deliberation.<sup>24</sup>

---

term human subject emerged in the context of research ethics in response to harmful treatment of persons in medical experiments, as discussed in detail in Section 5: Legal Frameworks in TIP Data Collection.

<sup>22</sup> English, A. (2017) 'Mandatory Reporting of Human Trafficking: Potential Benefits and Risks of Harm', *AMA Journal of Ethics*, 19(1), pp. 54-62. The same article notes that in the United States, several states have amended child abuse reporting laws to specifically include some or all forms of human trafficking.

<sup>23</sup> *A priori* knowledge or determination is that which is independent of experience or empirical evidence. By contrast, *a posteriori* knowledge is based on experience or empirical evidence.

<sup>24</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 13. See also Brunovskis, A. (2010) 'Irregular Migration in Norway' in Thomsen, T.L., et al. (Eds.) *Irregular Migration in a Scandinavian Perspective*. Netherlands: Shaker Publishing, pp. 47-49 and 65-68; Horning, A. and A. Paladino (2016) 'Walking the Tightrope: Ethical Dilemmas of Doing Fieldwork with Youth in US Sex Markets' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 205-226; Kelly, L. and M. Coy (2016) 'Ethics as Process, Ethics in Practice: Researching the Sex Industry and Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human*



In the current era of technology, the parameters of human subjects research are also being reconstituted, as noted by the Association of Internet Researchers:

If information is collected directly from individuals by email, instant message or an interview in a virtual world, we are likely to define this as research with a person (human subject). If the connection between the object of research and the person who produced it is indistinct, there may be a tendency to define the research scenario as one that does not involve persons.<sup>25</sup>

The Association goes on to note:

On-going debates illustrate a diverse, educated range of standpoints on the answers to the question of what constitutes a human subject. We agree with other regulatory bodies that the term no longer enjoys the relatively straightforward definitional status it once did. As a community of scholars, we maintain the stance that when considered outside a regulatory framework, the concept of human subject may not be as relevant as other terms such as harm, vulnerability, personally identifiable information, and so forth. We encourage researchers to continue vigorous and critical discussion of the concept of human subject, both as it might be further specified in internet-related research or as it might be supplanted by terms that more appropriately define the boundaries for what constitutes inquiry that might be ethically challenging.<sup>26</sup>

Questions, therefore, arise about the boundaries of human subjects research and other possible more useful framings. These questions persist in all fields of social science research. Specific considerations for TIP data collection are offered below and in relation to some specific categories of data collection that may overlap in practice.

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

Risks to human subjects may be higher when subjects are vulnerable. **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).<sup>27</sup>

The concept of vulnerability is relative and dynamic. While some countries recognize vulnerable statuses and offer certain protections in law, in other countries the legal

---

*Trafficking*. Switzerland: Springer International Publishing, pp. 33-50; Lewis, H. (2016) 'Negotiating Anonymity, Informed Consent and 'Illegality': Researching Forced Labour Experiences Among Refugees and Asylum Seekers in the UK' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 99-116; Marcus, A. and R. Curtis (2016) 'No Love for Children: Reciprocity, Science, and Engagement in the Study of Child Sex Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 191-204; Siegel, D. and R. de Wildt (2016) 'Introduction: The Variety of Ethical Dilemmas' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 1-4; and Zhang, S.X. (2016) 'The Ethical Minefield in Human Trafficking Research - Real and Imagined' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 85-98.

<sup>25</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 6 and pp. 9-10.

<sup>26</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 6 and pp. 9-10.

<sup>27</sup> IFCR (2017) 'What is vulnerability?', *Disaster and Crisis Management*. International Federation of Red Cross and Red Crescent Societies.

framework does not recognize or protect vulnerable persons. Vulnerability is most often associated with poverty, but it can also arise when people are isolated, insecure and defenseless in the face of risk, shock or stress. Vulnerability factors may also relate to belonging to a specific social group or to the individual's sex, gender identity, sexuality, ethnic or other identity, age or other characteristics.

**Definition. Vulnerable persons<sup>28</sup>**

Individuals who are relatively (or absolutely) incapable of protecting their own interests. They may have insufficient power, intelligence or education, resources, strength or other needed attributes to protect their own interests.



Some laws require special measures to be taken where vulnerability factors are present in data collection. Photograph by Peter Biro.

Trafficking victims may be considered vulnerable persons as victims of the crime of trafficking in persons. Experts have explained vulnerability in trafficking contexts as relating to personal, situational or circumstantial factors. As examples, **personal vulnerability** may relate to physical or mental disability; **situational vulnerability** may relate to a person's marginalization based upon ethnicity, imposed statelessness or ineligibility for national citizenship (in law or unofficially), irregular status or physical, social or linguistic isolation; and **circumstantial vulnerability** may relate to a person's poverty, living in a

<sup>28</sup> Definitions of vulnerable persons vary across jurisdictions and legal instruments, as well as according to the purpose for which the term is being used. The general definition provided here draws from CIOMS (2016) *International Ethical Guidelines for Health Research involving Humans*. Geneva, Switzerland: Council for International Organizations of Medical Sciences, Guideline 13. Examples of vulnerable groups include people receiving welfare benefits or social assistance and other poor people and the unemployed, patients in emergency rooms, some ethnic and racial minority groups, homeless persons, nomads, refugees or displaced persons, prisoners, patients with incurable disease, individuals who are politically powerless and persons who have serious diseases.

conflict zone or being held in detention. These vulnerabilities can be pre-existing or can be created by traffickers or trafficking experiences.<sup>29</sup>

Data collected for administrative purposes may be collected on the basis of a vulnerability factor (for instance, health data that is collected about a particular condition or disease or immigration data collected on the basis of irregular status). A framework generally governs how that administrative data is to be collected from a data subject (for example, in the medical, immigration, criminal justice or other contexts in which data collection with vulnerable persons is carried out). However, when data is collected in the context of trafficking or related research, a specific framework will need to be put into place to ensure that data subjects, as vulnerable persons, are protected from any potential harm due to the collection of data or its use. As one NGO researcher reflected:

...one of the big [ethical principles] is the “do no harm” concept. These are [human subjects] that may either be vulnerable, may actually be in exploitative and abusive situations, or may be recovering from abusive and exploitative situations. So, making sure that they are not re-traumatized, re-victimized, that’s one of the biggest challenges.

The focus and designation of vulnerability is very often on the vulnerability of trafficking victims themselves. However, in the context of trafficking-related data collection, vulnerability may not be confined only to the individual trafficking victim but might also apply to the victim’s family, friends, neighbors and community members. Further, in some cases, traffickers may also have vulnerable status, as individuals who have entered the criminal justice system as suspects or who have been convicted of a crime.<sup>30</sup> Persons who are involved in the criminal justice system may face specific vulnerabilities, including stigmatization as suspects of crimes irrespective of their guilt. Convicted persons who are incarcerated may be in a weakened position to give meaningful consent, feel pressured to participate (or to not participate) in research or data collection or face threats and influences during their participation.<sup>31</sup> Once released from prison, former prisoners commonly suffer economic disempowerment, restricted access to jobs and housing, stigmatization and discrimination. From a research and data collection perspective, the vulnerability of such persons can be acute, particularly when risks of retaliation persist if others involved in trafficking are not incarcerated. Moreover, as pressure mounts within the anti-trafficking field to increase prosecutions, there is a concern that the number of low-level criminals incarcerated for human trafficking will grow, offering researchers a captive pool of data sources.

Some laws require special measures when vulnerability factors are present in data collection.<sup>32</sup> And when a potential data collection subject is considered vulnerable or data collection involves vulnerable groups, specific ethical considerations are raised. Data collectors must ensure that the information provided to data subjects about the data collection effort is tailored to vulnerable persons and takes into account how best to

---

<sup>29</sup> UNODC (2012) *Guidance Note on “abuse of a position of vulnerability” as a means of trafficking in persons in Article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*. Vienna, Austria: United Nations Office on Drugs and Crime, point 2.3.

<sup>30</sup> Please see the discussion below on data collection involving suspects and convicted criminals, including human traffickers (Section 4.1.3).

<sup>31</sup> Because prisoners are vulnerable, there are additional protections attached to their involvement as research subjects. Government of the United States (2009) *Code of Federal Regulations*, Title 45, Part 46, Subpart C (“Federal Policy for the Protection of Human Subjects” or “United States Common Rule”).

<sup>32</sup> For example, in the United Kingdom, in situations where a vulnerable adult participant may be unable to make a fully informed decision, the Mental Capacity Act 2005 requires consultation with the participant’s caregiver(s). Reason (2015) *Ethics for Research with Children, Young People and Vulnerable Adults*. United Kingdom: Reason, p. 3.

approach informed consent.<sup>33</sup> One NGO, partnering with government counterparts to conduct research on traffickers, described the need to approach research with this population with care:

...it's very important to tell [the perpetrators that the] information [we collect from them] will not have any effect on their [criminal justice] process. [This data collection] is to understand and to be able to eventually help victims ... And of course, [their participation is] voluntary and so on... [In terms of legal issues], we have to get the permission of the prosecutors... This is research [being] done with the Ministry of Justice ... the idea is to [use] an approach that is not violent (forceful) with [the perpetrators] ...

Assessing an individual's competence can be difficult in some circumstances,<sup>34</sup> as is gaining meaningful informed consent.<sup>35</sup> For example, vulnerable adults may be concerned about signing a written consent form and consideration could be given to alternative strategies for obtaining legitimate verbal consent, such as by audio recording the consent process. Alternatively, an individual may be too immediately willing to consent to participate, without fully understanding the risks and ramifications of doing so. To the extent possible, vulnerable persons should be approached about research participation when they are at their least vulnerable. For example, a trafficked person who is currently being actively exploited may be more vulnerable than one who is in the process of recovery and has access to support.

Cultural factors are also important considerations when gathering data with vulnerable persons, especially when a data collector and data subject are from different backgrounds. Cultural attitudes regarding social hierarchies (for example, between data collector and data subject), respect for authority, gender roles, differences in age, and concerns about stigma may influence the potential subject's decision to accept or decline the research opportunity. These issues need to be addressed in a way that allows the data subject to give voluntary and informed consent.

For TIP data collection, the inclusion of a vulnerable group is generally only justified if the data collection is responsive to the needs and priorities of that group and cannot instead be carried out with a non-vulnerable group.<sup>36</sup> Therefore, in designing TIP data collection it is important to consider whether the inclusion of vulnerable human subjects is necessary to realize the objectives of the data collection initiative, as one TIP researcher noted:

---

<sup>33</sup> EU (2016) *Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* ("EU Directive 2016/680"). Brussels: European Union, paragraph 39.

<sup>34</sup> Informed consent can present particular problems when researching people with some levels of learning disability, those with dementia or diminished cognitive ability or sense of self, including individuals experiencing mental ill-health or people under the influence of drugs. Reason (2015) *Ethics for Research with Children, Young People and Vulnerable Adults*. United Kingdom: Reason, pp. 2-3.

<sup>35</sup> Voluntary and informed consent refers to the process by which data subjects voluntarily agree to take part in data collection. This requires a clear understanding of what participation entails, including the potential risks and benefits, and then making a decision to participate without coercion. Gaining informed consent requires, at minimum, the following information be provided to respondents/participants: the purpose of the data collection including the specific topic; who is involved in the data collection and will have access to information/data; potential risks and benefits of participating; how confidentiality and anonymity will be maintained; and how, where and with whom the information will be used, shared and presented.

<sup>36</sup> WMA (1964) *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects*. Helsinki: World Medical Association ("Helsinki Declaration"), paragraph 20 and CIOMS (2016) *International Ethical Guidelines for Health Research Involving Humans*. Geneva, Switzerland: Council for International Organizations of Medical Sciences ("CIOMS Guidelines"), Guideline 13.

There is an ethical obligation to ensure that if you're going to work with vulnerable populations, then it needs to be justified by the research question.

Examples of when this might be the case would include when data collection is intended to inform policy and program responses to: prevent trafficking of a particular group; better assist trafficking victims from among that group; empower vulnerable persons (for example as partners or through participatory research); and/or to collect data that vulnerable persons have asked for or to try to answer questions that they have posed. However, even when the inclusion of the group is justified, there may still be research questions and data collection projects where it is preferable not to include vulnerable persons as data sources.

Another consideration in the design of TIP data collection is that, to the extent possible, the data subjects selected should be the least vulnerable while fulfilling the purposes of data collection. It is important to consider whether the inclusion of vulnerable human subjects is necessary to realize the objectives of data collection. For instance, a study that concerns the trafficking of vulnerable persons may be able to obtain useful data from respondents who are not vulnerable persons themselves, but who come into contact with vulnerable persons (such as family members of trafficking victims, social workers, and others who work with victims rather than victims themselves). This consideration reveals the particular challenges for organizations and institutions whose work necessarily involves vulnerable populations, including victims of trafficking or children or incarcerated persons. Ethical challenges are acute when data collection is carried out with persons who are primarily beneficiaries (to whom the assisting NGO or state owes a duty of care) but are also research subjects or potential sources of data.



In designing TIP data collection, it is important to consider whether the inclusion of vulnerable human subjects is necessary to realize the objectives of data collection. Photograph by Peter Biro/ECHO.

Whether the group about whom data is collected stands to benefit from knowledge, practices or the interventions that result from the collection of data is also important in making a determination about their participation. As one trafficking researcher explained:

I think that we need to think much more carefully about participation and, by that, I mean not only that people have a say in the kind of instrument that you're using or the approach that you are [taking] but also that people really benefit from the research.

Examples might include research about services for trafficking victims aimed at improving the services that they receive or a study of stigmatization of certain categories of vulnerable persons that results in the design of interventions to reduce stigmatization and improve reintegration of research participants into their communities.

This notion of benefit relates to the wider ethical principle of “do no harm”.<sup>37</sup> When including a vulnerable group in data collection, attention is needed to the principle of “do no harm”, including carefully considering what data is needed (and what may not be needed). One researcher described the importance of making ethical judgments to “do no harm” when carrying out TIP data collection:

There are certain ethics and questions that you need to [consider to] make sure you don't re-traumatize the victims. So, if I'm doing program evaluation work and I want to get the victims' perspectives on the program, it's making sure [the] questions [I ask them] relate to the services that they received from the program within those parameters. I don't necessarily need to hear their trafficking story, for example.

In some situations, it may 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. Doing so may even be discriminatory and amount to denying the individual an opportunity for their voice to be heard as well as the opportunity to partake in the benefits of participation.<sup>38</sup> When inclusion of vulnerable persons in data collection is considered justified, extra protection mechanisms will likely be warranted in order to ensure that participants are protected before, during and after data collection. Data collectors will need to scrutinize the quality of consent processes for vulnerable individuals and put into place measures to mitigate identified risks.

Children are considered a vulnerable group and, in addition, many children will have their own additional vulnerabilities. As one TIP researcher explained, additional justifications and protections will therefore apply:

There's a whole set of guidelines for what justification you need to do research involving children, what protections you have to have in place.

Specific and complex legal and ethical issues must be considered when engaging children in research or data collection. For example, consent requirements are significantly different in the case of children than adults. Children's involvement in a given research or data collection activity usually requires specific and additional procedures and approvals. One TIP expert specialized in child protection described data collection projects with children which did not adequately take ethics into account:

---

<sup>37</sup> See United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1978) *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Bethesda, United States: National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (“Belmont Report”).

<sup>38</sup> Brunovskis, A. (2010) ‘Irregular Migration in Norway’ in Thomsen, Trine Lund, et al. (Eds.) *Irregular Migration in a Scandinavian Perspective*. Netherlands: Shaker Publishing, pp. 48-49.

I have seen cases when children have not been taken through the full list of information [for informed consent] and I think that is really unethical. How is it ethical to involve someone in a more difficult, fragile position than you and not really inform them of the whole process? What will be the use of the data? Will you be recording or not? [Ethical research requires that you provide] all of the information that you need for someone to feel comfortable in taking part in an interview.

Application of the principle of “do no harm” in TIP data collection with children means ensuring the “best interests of the child”. Securing the “best interests of the child” means that the needs and interests of the child supersede any need to complete an interview or data collection activity. Guarding the “best interests of the child” in data collection involves balancing key factors related to the competing rights of the child: the views of the child; the views of family members and others close to the child; safety as a priority; the importance of the family and of close relationships; and nurturing the development needs of the child. One child protection specialist stressed the importance of a clear understanding of child protection issues when undertaking data collection with and about children:

If you’re working with children and young people, a really clear understanding of child protection issues, possible ethical issues related to children and young people is something that’s key. Assuring that risk assessments and everything else has been undertaken.

A primary consideration is to guard against emotional or physical harms and protect a child’s rights and interests. Because children may not be well-equipped to raise concerns associated with their involvement in data collection, data collectors should consult with children and also family members or guardians. It may also be necessary to consult local stakeholders. Some countries have laws and regulations applicable to data collection with children. When ethical guidelines are in place in a given context, specific considerations are generally provided for the involvement of children in research. Additionally, there is some guidance available at the international level that can be applied to data collecting involving trafficked and exploited children. For instance, the United Nations Children’s Fund (UNICEF) *Guidelines on the Protection of Child Victims of Trafficking*, includes a brief section on ethical principles when doing research on child trafficking. Central ethical considerations include: whether the research is necessary and requires the involvement of children; whether children may be harmed in referring to past experiences; whether there are any potential risks (physical, psychological, social or emotional) to the children; who is the best person to approach children; whether results have the potential for harm or stigma to children; whether results will benefit children; and so on.<sup>39</sup> There may also be power dynamics that come into play around differences in race, ethnicity and other social signifiers of both the child-respondent and those involved as data collectors and gatekeepers, although this is not unique to data collection involving children.

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 approaches that are culturally sensitive, rights-based and trauma-informed.<sup>40</sup> Additional skills will be needed when engaging children in research. It is important to ensure that child protection

---

<sup>39</sup> UNICEF (2006) *Guidelines on the Protection of Child Victims of Trafficking*. New York, United States: United Nations Children’s Fund, p. 37. See also Berman, G. et al. (2016) *What We Know about Ethical Research Involving Children in Humanitarian Settings: An overview of principles, the literature and case studies*. Florence, Italy: UNICEF Office of Research – Innocenti; and UNICEF (2003) *Principles and Guidelines for Ethical Reporting: Children and Young People under 18 years old*. New York, United States: United Nations Children’s Fund.

<sup>40</sup> A trauma-informed approach involves understanding the physical, social and emotional impact of trauma on the individual and incorporating victim-centered practices into TIP data collection.

measures are built into data collection initiatives, which means all staff involved in data collection with children (including translators, assistants and administrative staff) should:

- have experience and knowledge of working with children and be trained in child protection principles;
- be trained in trauma-informed approaches to data collection;
- be screened for their appropriateness in working with children;
- be aware of the local legal and social welfare systems in place;
- be aware of the local social and cultural contexts;
- have information about support organizations/institutions in the local area and talk with these organizations/institutions about their accessibility and availability for referrals.

#### 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).<sup>43</sup> In TIP data collection, personal data is most frequently about trafficking victims.

There is a distinction to be made between single-case data and personal data. While single-case data can be either personal or non-personal, personal data is always identifiable.<sup>44</sup> An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.<sup>45</sup> An individual can be considered identifiable from the use of full names or a combination of identifying

##### **Definition. Personal data<sup>41</sup>**

Data that can be used on its own or with other information to identify a data subject. In broader terms, personal data is any information relating to an identified or identifiable person.

##### **Definition. Sensitive data<sup>42</sup>**

Personal data that requires additional protection because disclosure may have serious adverse effects on the individual and/or because it is specifically protected by law.

<sup>41</sup> Definitions of personal data vary across jurisdictions and legal instruments, as well as according to the purpose for which the term is being used. The general definition provided here draws from the GDPR, which states: “personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union (“General Data Protection Regulation” or “GDPR”), Article 4.

<sup>42</sup> Definitions of sensitive data vary across jurisdictions and legal instruments, as well as according to the purpose for which the term is being used. The general definition provided here draws from EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union (“General Data Protection Regulation” or “GDPR”), Article 9.

<sup>43</sup> The European Commission defines personal data as “any information that relates to an identified or identifiable living individual” and notes: “Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law”. EC (2018) ‘What is personal data?’, *Data Protection*.

<sup>44</sup> Data used for strategic and policy purposes in prevention, repression of trafficking-related activities and assistance may be non-case specific, anonymous and non-personal. Personal data, unlike non-personal, aggregated data, are subject to data protection regulations.

<sup>45</sup> EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union (“EU Directive 95/46/EC” or “EU Data Protection Directive”).



aspects such as physical characteristics, pseudonyms, occupation, address and so on.

Personal data might include, among other information, the name, date of birth, known address or whereabouts, telephone number and number of identity documents, which may be collected by NGOs and other victim service providers rendering services to trafficked persons or by police and prosecution services collecting data on traffickers for the purpose of investigation and prosecution.<sup>46</sup> As is discussed in Section 7: *Emerging Issues in TIP Data Collection*, in the era of Big Data and analytics, what constitutes personal, identifiable data is undergoing some change and debate.<sup>47</sup>

Some personal data is considered **sensitive data**, meaning that a breach of this data presents a greater risk to a person's private life than "regular" personal data and, therefore, requires extra protection.<sup>48</sup> For example, Article 9 of the European Union *General Data Protection Regulation* addresses sensitive data as "special categories of personal data" that include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".<sup>49</sup> Because this information is private and because these special categories of information could be used in a discriminatory way against an individual or even lead to the targeting of certain individuals, sensitive data should be treated with greater care and be subject to more stringent restrictions.<sup>50</sup>

**Personal data protection** forms the basis of the legal framework for data collection (privacy law), as discussed in Section 5: *Legal Frameworks in TIP Data Collection*. Legislation in different jurisdictions explicitly prohibits the collection of certain types of data that may have bearing on ethical considerations or require specific measures to be put in place for exceptional circumstances. TIP data collection that includes personal data raises specific legal and ethical concerns, as one NGO director elaborated:

At all times [we are] mindful of personal data privacy, of the risk of defamation, of the risk of any sort of breaches of law and just the physical security risk of providing information and where that might go... the same sort of rules always apply: checking personal data privacy, thinking about the ethics of it. What risk is there in a physical sense? What risk is there to organizations? What confidentiality have been put in place? Is there [a non-disclosure agreement]? If there isn't should there be one?

---

<sup>46</sup> Pesce, F. and I. Orfano (2009) 'Guideline 15', *Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators*. Vienna, Austria: International Organization for Migration and Federal Ministry of the Interior of Austria, pp. 43-44.

<sup>47</sup> This is discussed in more detail in Section 7.2 *Using Big Data in anti-trafficking work*.

<sup>48</sup> CoE (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108. Strasbourg, France: Council of Europe; and EU Directive 95/46/EC.

<sup>49</sup> EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union ("General Data Protection Regulation" or "GDPR"), Article 9. Similarly, Article 8(1) of the *EU Data Protection Directive* defines sensitive data as: "Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life". EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union ("EU Directive 95/46/EC" or "EU Data Protection Directive"), Article 8.

<sup>50</sup> The processing of sensitive data is allowable only in exceptional circumstances and with sufficient safeguards including that it has a legal basis; is necessary for reasons of substantial public interest; and is subject to suitable safeguards. EU Directive 95/46/EC.



All data collectors must be aware of and understand their different and various obligations, both legal and ethical, in terms of collecting personal data. Photograph by Peter Biro.

Every actor engaged in TIP data collection, whether a private organization (such as a charity or NGO), a government department or agency, an academic institution or an individual researcher, may engage in data collection that involves personal data. All data collectors should be aware of and understand the various obligations, both legal and ethical, in terms of collecting personal data. For example, the collection of personal data often takes place for administrative purposes and questions arise as to how to marry data protection obligations with the need for some personal data as part of operational work. NGO service providers assisting trafficking victims are required to collect personal data about beneficiaries to document the provision of services and to provide information to government and international donors to account for funds spent on assistance. Personal data from victims is also needed when, for example, victims register in the state system to access social assistance and healthcare. NGO service providers may also face an obligation to share information including personal data about their victim beneficiaries with law enforcement or other authorities. This could be discretionary, such as when cooperating in anti-trafficking efforts, or required by law (for example, for the government to issue a reflection period and/or residence permit). Similarly, NGO service providers may be required to share information about trafficking victims, including personal data, in their cooperation with a government institution or, in some cases, the country's National Rapporteur. One National Rapporteur explained how her office collected and stored personal data from trafficking victims:

This is not a [publicly accessible] database. We don't publish the names of the victims. We put the names in the database, but each name gets a code, so they are identified by code. The persons who have access in the database [have] a "security certificate" that we get from [the] Directory in the Prime Minister's office. So, everybody who gets to know secret information, confidential information, he's obliged according to the law not to publish it, not to do any harm with that. And the database is within a secure system of the state police, so [the public] cannot have access in it. But we do respect the data, the private data of the victims. It's a law that we have to obey.

### **Box #1. Breaches of confidentiality in administrative data**

In 2015, a London-based health clinic inadvertently leaked data on persons who had visited HIV clinics in the vicinity (a small area of London). The clinic disseminated an electronic newsletter to individuals who had opted-in to this online service, but instead of blind copying recipients, accidentally made all email addresses and most names of recipients visible.<sup>51</sup>

In 2017, an insurance company in the United States distributed letters to 12,000 of its customers living with HIV in which the HIV status of patients was visible in the plastic window of the envelopes.<sup>52</sup>

The collection of personal data for administrative purposes may involve the storage of personal data, including potentially the use of cloud computing services.<sup>53</sup> When personal data is collected and stored for administrative purposes, breaches of confidentiality can have serious consequences. While not in the context of TIP data collection, two illustrations of the potential for accidental leaks of sensitive data are discussed in Box #1. It is not difficult to imagine how similar leaks of personal and sensitive information about trafficking victims could likewise result in harm.

There have been instances in which trafficking victims have received sexual or mental health services from service providers and their data (collected in the context of this assistance) was made public to others, an example of which appears in Box #2 below.

### **Box #2. Leaks of sensitive personal data from administrative data**

One woman returned to live in her community after trafficking. She visited the local medical clinic, where she tested positive for HIV. Her HIV status was leaked by staff at the medical clinic, which meant that she and her son suffered serious discrimination: “When I came back, I tested positive for HIV at the local clinic. Then the whole village got to know it. My neighbors learned about it. I had very many problems. They didn’t let me approach the well. They treated me as if I were a piece of dirt. They humiliated me. I had many problems with my child at school. They wanted to expel him from school, although I showed them the negative result of his test, under different pretexts. I suffered a lot”.<sup>54</sup>

Criminal justice data also includes detailed personal information about suspected and convicted perpetrators, as well as victims of the crime of trafficking in persons as part of work on investigations and prosecutions. Here too, breaches related to human trafficking occur, constituting egregious violations of ethics and law. For example, in some instances law enforcement has provided the media with the names and addresses of trafficking victims who had filed complaints with the police and the media then contacted these victims in their home villages, as described in Box #3 below.

---

<sup>51</sup> Fox, C. (2016) ‘NHS trust fined for 56 Dean Street HIV status leak’, *BBC News*, May 9.

<sup>52</sup> Duffy, N. (2017) ‘Insurance giant accidentally leaked HIV status of thousands of patients’, *Pink News*, August 25.

<sup>53</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p. 17.

<sup>54</sup> Surtees, R. (2007) *Listening to Victims: Experiences of Identification, Return Assistance in SE Europe*. Vienna, Austria: ICMPD, pp. 201-202. In another study of victim assistance in Moldova, one formerly trafficked woman’s potential HIV status was disclosed due to mishandling of her personal information by health clinic staff. See Brunovskis, A. and R. Surtees (2007) *Leaving the past behind? When victims of trafficking decline assistance*. Oslo: Fafo and Washington, D.C., United States: NEXUS Institute.

### Box #3. Unauthorized release of personal data by police<sup>55</sup>

One trafficking victim described how police disclosed her full name, address and other personal information to journalists who then published a story about her, without her consent, leading to her being located by her traffickers in her home community and then harassed and threatened: “[The police officer] gave a statement to the press. There was my full name ... All newspapers were full of that: ‘Girl was pulled out from the criminal group. Name of girl is that. She lives there. Age that. She was married. She has son. Name of the son was...’ All newspapers were full of that [information]. I couldn’t believe that my story reached [the neighboring country]. I was shocked. I couldn’t continue... They harassed me at my house, they threatened me. Many things happened.”

One trafficked woman described how her details and address were given to local journalists without her knowledge or consent and how journalists then came to her home community to interview her: “Once the local policeman sent a group of journalists to my house. They came to take my picture. I asked them to leave me alone. At that moment my lawyer came and I asked him to help me get rid of those stupid journalists since he was my lawyer. He did nothing”.

One police inspector involved in the arrest of a group of traffickers provided information about the case to the news media. This included giving all of the details of where the trafficking victim in the case was living as well as photographs of her house. As she came from a small village, everyone immediately knew who the victim was.

One staff member involved in a data collection project described a situation when lack of personal data protection combined with corruption put trafficking victims at risk:

There were also [past] cases of misuse of data by corrupt police officers who then blackmailed certain victims and asked for sexual services in exchange [for] not disclosing information to their families, communities. So [in our project] we insisted really a lot on this principle of data protection.

There are also situations in which sensitive information is not adequately protected. One example was when case files of child trafficking victims were not stored securely in one government’s administrative offices but kept in the hallway because of a lack of storage space.<sup>56</sup> Other examples include situations in which NGOs have been pressured by police to hand over case files on persons who are receiving their assistance. These situations do not necessarily mean that personal data should not be collected; it may be necessary to collect personal data in order to effectively respond to TIP. Rather, these examples and scenarios highlight the importance of ensuring that any such data is also protected.

These are not uncontested issues and there are competing discussions around the collection of personal data within the TIP field. As the previous Dutch National Rapporteur observed, lack of access to personal data can compromise the ability to link datasets from different institutions and inhibit the ability to answer certain questions when “the answer to these questions could prove to be essential to evaluate the protection of victims”. Further, “...the protection of victims reaches out into the data gathering. The privacy of both victims and offenders should be protected. However, in my opinion, the protection of victims should outweigh the convulsive protection of the victim’s privacy”. Moreover, while recognizing the uneven political environments in which TIP data is collected and the higher risk of collecting personal data in some contexts, she also pointed to the need to explore how these two

<sup>55</sup> Surtees, R. (2013) *Ethical principles in the re/integration of trafficked persons. Experiences from the Balkans*. Washington, D.C., United States: NEXUS Institute and Brussels, Belgium: King Baudouin Foundation, p. 47; Surtees, R. (2007) *Listening to Victims: Experiences of Identification, Return Assistance in SE Europe*. Vienna, Austria: ICMPD, p. 171 and p. 201.

<sup>56</sup> Surtees, R. (2013) *Ethical principles in the re/integration of trafficked persons. Experiences from the Balkans*. Brussels, Belgium: King Baudouin Foundation and Washington, D.C., United States: NEXUS Institute, p. 77.

elements can be reconciled, which may need to be approached differently in different settings:

...in some countries revealing the personal details of [a] victim may prove hazardous for them in their country of origin. That is a grave factor to consider. Evidently. But there is a difference between getting the data and protecting the privacy and not getting the data at all and failing the victim in his or her protection.<sup>57</sup>



Personal data is often collected and stored for administrative purposes. Photograph by Peter Biro.

An emerging issue in terms of personal data is biometric data. The examples in Box #4 below illustrate how new technologies introduce new personal identifiers – like biometric data – that need to be included and considered when exploring the relevant protections. In some cases, this may be addressed by how the data is handled, processed and stored after being collected. This challenge of protecting data while needing to collect it (for example, as part of service provision) is not unique to trafficking and is part of a wider discussion when working with and collecting personal or sensitive data. An additional layer of complexity is introduced when considering what constitutes privacy in different countries, cultures and even for different individuals.

One data collection project staff member noted the difficulty in working with partner organizations that approach privacy and confidentiality differently:

---

<sup>57</sup> Dettmeijer-Vermeulen, C. (2013) *National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children in the Netherlands*. Berlin, Germany: Data Protection and the Right to Privacy for Marginalised Groups - A New Challenge in Anti-Trafficking Policies Conference.

[Our partner organizations] really don't understand or see the confidentiality issues in the same way that we see them [at our organization] ... We consistently receive reports [from our partner organizations] with photos, identity documents photocopied into them, names, birthdays, birth villages... So, there isn't really contextually an understanding of the need for confidentiality of data within our partner organizations and I would say arguably by the [data subjects] themselves. There is this sense that if you are accessing one of these services, you're out in the public realm. And I'm not saying that excuses not having appropriate... storage and confidentiality frameworks. But it does make it particularly challenging because we keep sending reports back saying, "Please blank out all personal details" and they keep coming back with more personal details.

**Box #4. Biometric data from migrant workers<sup>58</sup>**

The member states of the Gulf Cooperation Council (GCC) are developing a joint database to enable biometric data (that is, fingerprints and iris scans) to be shared between GCC countries to track migrant workers' health and prevent convicted migrant workers from re-entering any GCC state.

The government of Thailand has started collecting biometric data (iris scans, with plans for facial and fingerprint scanning) to register migrant workers working on fishing vessels to address human trafficking in the Thai fishing industry.

Another staff member from the same data collection project noted that the challenges around differing understandings of personal privacy seem to be particularly acute in countries with current or former authoritarian governments:

It is often far outside the mindset of both service providers and beneficiaries in these countries to consider that there is a right to privacy to be respected during data collection.

This experience aligns with a conclusion that researchers have reached more generally on the contextual nature of these discussions. That is:

Individual and cultural definitions and expectations of privacy are ambiguous, contested, and changing. People may operate in public spaces but maintain strong perceptions or expectations of privacy. Or they may acknowledge that the substance of their communication is public but that the specific context in which it appears implies restrictions on how that information is – or ought to be – used by other parties.<sup>59</sup>

Moreover, 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. As such, data collection in such shifting terrains benefits from the concept of "contextual integrity", which serves as:

...an alternative benchmark for privacy, to capture the nature of challenges posed by information technologies. Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it.<sup>60</sup>

<sup>58</sup> AFP (2018) 'Thailand to scan eyes of workers in notorious seafood industry', *Geo Television*, February 15; Planet Biometrics (2015) 'Gulf countries move towards integrated biometric database', *Planet Biometrics*, February 9; and Spenser, T. (2012) 'GCC to fingerprint, iris scan migrant workers for health purposes', *Biometric Update*, October 9. The GCC member states are Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and United Arab Emirates.

<sup>59</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 7.

<sup>60</sup> Nissenbaum, H. (2004) 'Privacy as Contextual Integrity', *Washington Law Review*, 79.

There are also important questions to be asked about what constitutes personal data and the potential ways it can be accessed in the age of advancing technologies and Big Data.<sup>61</sup> That is, can a person be wholly removed from large data pools? Can data be used to single out a unique individual by applying existing and readily accessible means and technologies? Is there the potential that de-identified data (that is, where personal identifiers like name, date of birth, location, etc. have been removed), while not directly linked to an individual or group of individuals, may still single out an individual or group of individuals with the use of adequate technology, skills, and intent?

#### Some questions on personal data in the age of advanced technologies

- ② Can a person be wholly removed from large data pools?
- ② Can the application of technology single out a unique individual?
- ② Can an individual's identity be extracted from de-identified data?

For example, as noted by the Association of Internet Researchers, a data set containing thousands of tweets or an aggregation of internet surfing behaviors collected from a bot<sup>62</sup> may seem far removed from the persons engaged in these activities, leading one to overlook that these persons may be directly or indirectly impacted by the research. But the Association stresses: “there is considerable evidence that even ‘anonymised’ datasets that contain enough personal information can result in individuals being identifiable”.<sup>63</sup>

Concerns also exist regarding the role that technology can play in yielding personal data and the risk that such technology can be based on discriminatory grounds and used for discriminatory purposes. For example, a recently released research study using facial recognition technology was able to determine an individual's sexual orientation with a high degree of accuracy,<sup>64</sup> revealing the potential for some technology to produce sensitive data. Another recent study analyzed whether technology could detect criminality through facial features.<sup>65</sup>

Questions also emerge from the sharing of personal data through technological tools such as smart phone applications (apps), given recent enthusiasm in the anti-trafficking field to produce apps, which, in many cases, collect information about migrant workers and trafficking victims. It is not clear to what extent users (migrant workers and trafficking victims) are fully informed about and have meaningfully consented to the sharing of their personal data. Even when users provide their own data, as is illustrated in Box #5 below, they may not be able to anticipate the ways in which that data will be used, and by whom (for example, by law enforcers and immigration officers tracking irregular migration). One recent

---

<sup>61</sup> As noted above, “Big Data” is defined by the UN as “extremely large datasets associated with new information technology and which can be analyzed computationally to reveal possible patterns, trends and correlations”. OHCHR (2016) *A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance Note to Data Collection and Disaggregation*. Geneva, Switzerland: Office of the United Nations High Commissioner for Human Rights, p. 12 at fn 25.

<sup>62</sup> A bot is an application that performs an automated task. In this instance, a bot refers to a search engine application that crawls the internet to collect and aggregate search activities (“surfing behaviors”). Mitroff, S. (2016) ‘What is a bot?’, *CNET*, May 5.

<sup>63</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, pp. 10-11.

<sup>64</sup> See Burdick, A. (2017) ‘The A.I. “Gaydar” study and the real dangers of Big Data’, *New Yorker*, September 15 and Leetaru, K. (2017) ‘AI “Gaydar” and How the Future of AI will be Exempt from Ethical Review’, *Forbes*, September 16.

<sup>65</sup> Broad, E., A. Smith and P. Wells (2017) *Helping organisations navigate ethical concerns in their data practices*. United Kingdom: Open Data Institute, p. 17.

### **Box #5. Sharing of personal data through smart phone applications<sup>66</sup>**

IOM's MigApp is a free downloadable app that provides migrants with current, practical information about assistance. MigApp also facilitates data collection via online registration and storage of data captured through registration. Migrants can share their personal data as well as personal stories and photographs within the app.

Airline Ambassadors International (an airline industry charity) has developed a mobile "TIP Line" app, by which airline attendants can map their location, upload photos and videos and send text messages to be shared with designated authorities about possible human trafficking cases.

study on data sharing via mobile apps found that a significant proportion of apps share data from user inputs with third-parties, including personal information and without requiring a notification to the user.<sup>67</sup> In some cases, ensuring the security of sensitive data requires that the same level of protection be applied to de-identified data as explicit personal data. It is advisable 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.<sup>68</sup>

Factors that influence the likelihood of re-identification include availability of expertise, costs, amount of time required for re-identification and reasonably and commercially available technology. This also needs reconsideration regularly over time given that technological developments are fast moving and unpredictable.

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

While data on convicted criminals usually falls under exceptions to data protection laws,<sup>69</sup> it is important when collecting data on human traffickers to determine if and how some protections differ in the case of suspected as opposed to convicted criminals. Collecting data about persons suspected or accused of crimes (prior to a conviction) involves specific legal considerations, including privacy and confidentiality. For example, in the EU context, where data relates to offences, criminal convictions or security measures, data collection must be carried out only under the control of official authorities or safeguards specified by national law.<sup>70</sup> Legal and ethical issues in data collection with and about traffickers will be informed by the stage of the criminal justice process at which data is being collected. Suspects of the crime of trafficking in persons must be afforded the same rights and protections as victims of trafficking until the stage at which they are convicted of a crime definitively (that is have no further right of appeal).

Some privacy laws make it illegal to divulge certain types of information to anyone outside of the criminal justice system regarding a case that is a prosecutable offense. For example, certain laws set forth that names and other identifying information about suspects of a crime

<sup>66</sup> IOM (2017) 'Migrant Application (MigApp)', *ITC News*, January 16; and Rivard, N. (2015) 'New "TIP" Line App', *Airline Ambassadors International*, September 19.

<sup>67</sup> Zang, J. et al. (2015) 'Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third-parties by Mobile Apps', *Technology Science*, October 30.

<sup>68</sup> UN Global Pulse (2016) *Data Innovation Risk Assessment Tool*. United Nations Global Pulse, p. 73.

<sup>69</sup> Surtees, R. (2009) *Anti-Trafficking Data Collection and Information Management in the European Union - a Handbook. The situation in the Czech Republic, Poland, Portugal and the Slovak Republic*. Vienna, Austria: International Centre for Migration Policy Development, p. 56, noting that: "...the same privacy stipulations do not apply as 'convicted criminals' generally fall within the exceptions with regard to data transmission".

<sup>70</sup> EU (2016) *Directive 2016/680 on the protection of data of natural persons with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data*. Brussels, Belgium: European Union ("Data Protection Directive for the Police and Criminal Justice Sector"). The Directive ensures the protection of personal data of individuals involved in criminal proceedings, be it as witnesses, victims, or suspects.



are prohibited from being shared in order to protect their privacy and the integrity of on-going investigations. Further, witness statements and their contents may be governed by rules about non-disclosure to third-parties who have no legitimate interest in a case. As one criminal justice expert noted of his experience in cooperating with TIP data collection and research efforts:

...legally there could be real problems in terms of not only getting the information, but then, once you get the information, can you publish it in any kind of form that would be useful to outsiders without overstepping the law of that country? ... Criminal justice files, criminal files, criminal investigative files, we could not disclose them to interviewers from the outside without a waiver... And I remember being approached by [researchers] who would want to talk to us about our files and our investigations and as head of the office, my initial reaction was, “We can’t do that, it’s against the law”.

This prohibition may conflict with a data collector’s ethical course of action, compromising their ability to disseminate information in a way that benefits a data subject or community or even inhibiting the ability to provide appropriate access to assistance to people who need it. In such situations, stakeholders have developed different strategies to legally gain access to data that can benefit the anti-trafficking response. For example, the same criminal justice expert explained that access might be possible when data is collected and used internally or with specific restrictions that render the data collection legally allowable:

Under [one project] we did get access to files in many countries... And this was purely on the basis of the fact that we had built a good deal of trust [with authorities over time] and also we told them we wouldn’t publish it, that this would only be useful internally, for their internal review.

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 less onerous, the risks involved in sharing information – or not sharing it – in the particular country context will require balancing the interests of data subjects against 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. In some cases, a data collector could be subpoenaed to provide it and face legal issues for failing to provide such information. As one researcher explained:

You can apply for [an exemption to subpoenaed information]. But under the most rigorous laws, even that can’t hold up. There are potential issues about whether courts can go after certain [research] data.

In some cases, there may be a risk of retaliation against a data collection subject or data collector whether or not a person on trial is convicted. Where an accused person is not convicted, for example, they might seek retribution against the person who made the accusation. Or even when a person is convicted of trafficking in persons and incarcerated, they may still have connections to people who can retaliate. 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.

In such situations, what is legal may conflict with what is ethical, placing data collectors in situations that can have profound bearing on the safety of a data subject and others, including 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 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, issues may also arise in 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 permitted to share information about their anti-trafficking work. One criminal justice expert explained that the restrictions in such cases may apply both to key informants and the data collectors:

What could be quite serious is if a researcher does obtain information from a criminal justice practitioner and then publishes that information. It's possible that under the national law of a particular country that researcher could be liable under their laws for breaching the privacy act and can be prosecuted in that country. ...when I was in [one country], for example, I was working with prosecutors and investigators and they made it clear to me that they could not actually show me the files or provide me with details of the investigation unless I were to sign an agreement that should I then disclose that information outside the criminal justice arena in any kind of report or publication or even verbally outside the criminal justice system of that country that I would be subject to their criminal procedures.

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 and, thus, in a position to provide relevant information.

Those working in more constrained political contexts may not be able to safely participate in data collection that may yield negative findings (for example, failures of a country's anti-trafficking response, evidence of corruption). Key informants in such cases may risk reprisals. As one TIP expert observed of his data collection experience in one politically restrictive country:

We had an unfortunate incident in [one country] where we had reason to suspect that our room was bugged when we were talking to the NGOs. But that's because [some of the countries where we collect data] ... they're not exactly model democracies.

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<sup>71</sup> and may face risks when involved in data collection. As one researcher explained:

---

<sup>71</sup> A data source differs from a data provider, which is the individual or entity providing access to the data source.

There's a huge number of questions around the ethics of doing work with people who are dealing with people that were trafficked... Do you ask [the police] about corruption even though you know it's happening? Or [if you're interviewing staff from an] NGO providing services to the [trafficking victims in that country], do you ask them about corruption? Or does that put them at risk because they're worried about saying something, that if it gets out they're in trouble.

One criminal justice expert described a research study about the criminal justice response, which resulted in risks to criminal justice actors as key informants:

We hired people to collect data in certain countries... actually interviewing victims, interviewing public officials, doing more than just numbers, and then do an analysis of that [data] in a narrative form. But the issue then became: is this going to be made public in any way? And the problem was twofold. One, there were promises made during the interview session that it would not be made public and, two, there was serious concern and legitimate concern that if the information and the sources were to be made public in any way, there could be serious consequences for the people in that country in terms not only of their jobs, but even [in terms] of their safety. And it became a quandary of what to do. So, I think it is an ethical concern that data collection, specifically if it involves interviewing people and talking to people, there has to be a clear understanding at the beginning of the extent to which such information will be in any way published. And then there has to be a strict adherence to those promises and understandings.

Another potential concern when data collection involves anti-trafficking professionals as key informants is that the data may be skewed if it is filtered through the lens of particular political agendas or other interests. This can manifest for instance, in migrant sex workers being misidentified as victims of human trafficking, or in prosecutions of low-level criminals for serious human trafficking offences in a bid to inflate numbers reported. The result can be to weaken both the quality of data collected and the anti-trafficking response.

In short, when anti-trafficking professionals are data sources and data providers for a data collection project, there may be legal and ethical issues including risks. These may be more or less serious depending on the specific research project or the country or context in which data collection takes place. The types and extent of risk involved in data collection with anti-trafficking professionals as key informants need to be carefully considered and communicated to potential data subjects, consistent with voluntary and informed consent. At the same time, a disproportionate focus on research protections may curtail reasonable approaches to enhance the TIP knowledge base. The response to the existence of risk described in this subsection should not be to set extreme limits on data collection in this field. 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. As the director of one NGO suggested:

[In] any of this data collection, people [should] sit down and think about a solid framework to set out their policies... Then you also want to consider obviously what your ethical positions on things are, which hopefully are higher than the legal and the compliance side of things.

One National Rapporteur emphasized the importance and complementarity of these two elements in the data collection undertaken by her office:

First of all, I'm a public officer, so all of the secrecy, legal secrecy and provisions, they apply to me... I'm not able to reveal information on individual cases to anyone. And when I work with the issues of cases or case studies, I anonymize how it is said...I think about the ethics. We are human rights actors. And I think that human rights are really at the heart of the whole work we are doing. So, whatever we do, is always from the victim's point of view and what kind of questions, for example, we raise.

Ideally, legal and ethical requirements should align and be mutually reinforcing. However, this is not always the case. For example, it may be legal to collect TIP data, but doing so may not always be ethical. As one NGO service provider in Latin America explained:

I am always worried about the victim. ...there is a tendency to use victims for research, use victims for the media, use victims to do prevention, to...sensitize the people and so on. I can understand that maybe some adults or people who were victims are ready for that. But I really think there is an ethical issue in that that has to be solved and we have to address that more.

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 this protection. Concerns have been raised, for example, that inspection requirements may be used by a government to gain access to personal data using the very law that is meant to protect data subjects (although we did not encounter any such cases). Similarly, concerns exist that laws to protect personal data (privacy laws) could be used to undermine internet access and freedom of speech.<sup>72</sup>

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. Harm may also be caused by data collection protocols, tools or staff that are emotionally invasive or are carried out without fully informed consent, even if those 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 ethical. The political environment in which the data collection takes place must be factored in. One staff member of a data collection project described one country where this was a challenge:

...the concept of data protection... at that time it was a big issue and that's why many NGOs were not so eager to do this [data collection] exercise together with national institutions. [...] the level of corruption was pretty high also. There were also [past] cases of misuse of data by corrupted police officers who then blackmailed certain victims and asked for sexual services in exchange [for] not disclosing information to their families [and] communities.

---

<sup>72</sup> Mendel, T. et al. (2012) *Global Survey on Internet Privacy and Freedom of Expression*. France: UNESCO.

What is legal and what is ethical may come into particular tension in the case of constrained political systems where data collectors may not have legal freedom to conduct data collection. Equally in such political systems, 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 technically be 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. Conflicts between ethical standards and legal requirements may arise in situations where data collection may divulge information about an illegal activity. The legal obligation to report a crime may conflict with the ethical standards of confidentiality and protecting respondents from harm. As one researcher explained:

[Ethical considerations should include what] kinds of questions are being asked [of respondents]. If they answer certain information like, “I don’t have documentation”, would that information be creating risk that they would be liable for? [Researchers should also consider implications for] legal action. What if they’re reporting a context of abuse? Does that mean we have to report to a local authority? [If they answer], “I was beaten yesterday on my job”, how do we deal with that? In some contexts, [if] a researcher is given that information, particularly for child abuse or other forms of evidence of immediate abuse, that may be a reportable offense. You’d have to breach confidentiality to report that offense. But what if that offense went unreported, subjecting the person to additional harm, like deportation? So, all that stuff has to be vetted. ...and it often it’s quite long and lengthy conversation back and forth with the study team.

Similarly, another researcher highlighted that some disclosure during data collection may have legal obligations that contradict ethical assurances like confidentiality:

If you think you’re collecting information about someone’s experiences of trafficking, but within that they then share that they’ve been involved in some criminal activity or something else that’s not related to what you expected, [it is important to consider] how you deal with those disclosures. And being aware that actually some of the evidence you collect could be subpoenaed is something that is worth being aware of.

From a legal point of view, collecting data from human subjects who are engaged in activities that are illegal under the laws of the relevant country may expose data collectors themselves to risk of prosecution or other legal risks. As one researcher noted:

It depends on the country what the obligation of researchers are, in terms of the obligation to report crimes, information about crimes that have already taken place. It’s an underestimated issue. And of course, it’s different between countries, how obligated researchers are to report crimes they come across. Trafficking is a very serious crime so to come across the crime of trafficking and walk away, in many countries, this can be charged [under] criminal law. In the criminal code [of my country] it is an obligation for citizens to report serious crime to the police and as a researcher I sometimes break that law. ...many countries have obligation to report serious crime to the police which doctors and lawyers are exempted from, but not researchers. [...] I have been summoned to court to testify in concrete cases that the police suspect I have information on and, by law, I am under an obligation to testify.

As the above researcher highlights, 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. For example, in countries where prostitution or the purchase of sexual services is illegal, legal issues may arise where data is collected about vulnerability to human trafficking among persons in prostitution.<sup>73</sup> Another example, as noted above, is when laws mandatorily require healthcare professionals and others to report suspected trafficking victims to government health care and human services departments, as is the case in some states in the United States.

In some jurisdictions, the law requires confidential information to be released to relevant authorities, such as instances of child abuse. Compliance with such laws may raise risks to trafficking victims, particularly when their implementation does not adhere to ethical consent procedures and results in security breaches. This, as one researcher explained, can lead to important and otherwise ethical research and data collection not being undertaken:

...often the result is that people just don't do the research because they're not going to get permission [from an ethics review board] and they don't want to be in a position of violating the confidentiality agreement or violating a legal obligation to mandatorily report.

Given these myriad and inevitable legal and ethical grey zones in much TIP data collection, it is important to encourage discussion of these complex and conflicting issues. As noted in guidance from the Association of Internet Researchers' (AoIR) Ethics Working Committee:

Ethical conundrums are complex and rarely decided along binary lines. There is much grey area in ethical decision-making. More than one set of norms, values, principles and usual practices can be seen to legitimately apply to the issue(s) involved. It becomes difficult to make judgments as to which set(s) apply, especially when one set conflicts with another in some way. This forces the researcher to determine which is more relevant in a given context or at particular junctures during the course of the study.<sup>74</sup>

The complexity around ethical TIP data collection requires predicting outcomes and consequences of action in complex social and political landscapes. This complexity must not discourage discussion and reflection of these issues, but rather encourage and facilitate the ethical and legal conversations that can deepen understanding. The risk of being too rigid is that researchers and data collectors may stop doing ethically complicated research and data collection, not least with vulnerable persons. This can only have negative consequences for our ability to respond effectively (and ethically) to the issue of TIP, including in the aid of persons vulnerable to it. Moreover, that vulnerable persons would not be represented in TIP research and data collection is in and of itself a serious ethical concern.

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 *not* to conduct such data collection and research. One researcher highlighted such tensions surrounding data collection:

---

<sup>73</sup> In the case of TIP-related data collection, several examples of illegality may arise, for instance, because of the form of exploitation (prostitution, drug-related work, begging, criminal activities) or who is performing it (for instance, where minors are involved in work they should not be doing or gay sex is involved in a country where homosexuality is prohibited).

<sup>74</sup> The recommendations go on to stress the need for flexibility and contextualization: "We advocate guidelines rather than a code of practice so that ethical research can remain flexible, be responsive to diverse contexts and be adaptable to continually changing technologies. When one considers that ethical assessments are always operationalized via some sort of practice (method), and also contextualized institutionally and/or geographically, it becomes clearer that an adaptive, inductive approach can yield potentially more ethically legitimate outcomes than a simple adherence to a set of instantiated rules". Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 5.

I think the biggest ethical issue [we have faced] is probably the studies that we've been doing with street working children. ...it's a very unique population of children. We find this double-edged sword...where you have the ethical issue of asking questions that children might be uncomfortable with, that might be traumatizing... But then, at the same time, we have also the corresponding... ethical issue of working with a population that anecdotally is known to be highly susceptible to physical, sexual, emotional violence and [they] are not asked questions about it [to inform interventions].

Although blanket generalizations cannot be made as to what the most appropriate approach is in ensuring legality and ethics are properly addressed, 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. It is not tenable to select a research or data collection location to avoid rigorous ethical oversight, protection measures and legal requirements; a person should not receive fewer protections by virtue of the fact that the country where they are located does not have rigorous systems in place for the protection of data subjects.<sup>75</sup> Rather, in the design of research and data collection activities, the goal should be to ensure that legal and ethical protocols are in place and that data subjects are protected according to international standards and good practice, even where onerous burdens and sometimes creative measures are required to achieve this.

In short, TIP data collection must balance the need to comply with laws on the one hand, while ensuring that data collection is ethical on the other, including by protecting the rights and interests of data subjects as well as data collectors. Questions about what constitutes legal *and* ethical data collection are pressing in light of the global push for more data on human trafficking. The relationship between what is legal and what is ethical can be complex and varies by country and context. And each data collection project faces its own specific legal and ethical issues. 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. In other cases, the exact same course of action may expose stakeholders and data subjects to significant risks. Thus, 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.

---

<sup>75</sup> See Helsinki Declaration, Principle 10, which states: "Physicians must consider the ethical, legal and regulatory norms and standards for research involving human subjects in their own countries as well as applicable international norms and standards. No national or international ethical, legal or regulatory requirement should reduce or eliminate any of the protections for research subjects set forth in this Declaration". WMA (1964) *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects*. Helsinki, Finland: World Medical Association, Principle 10.

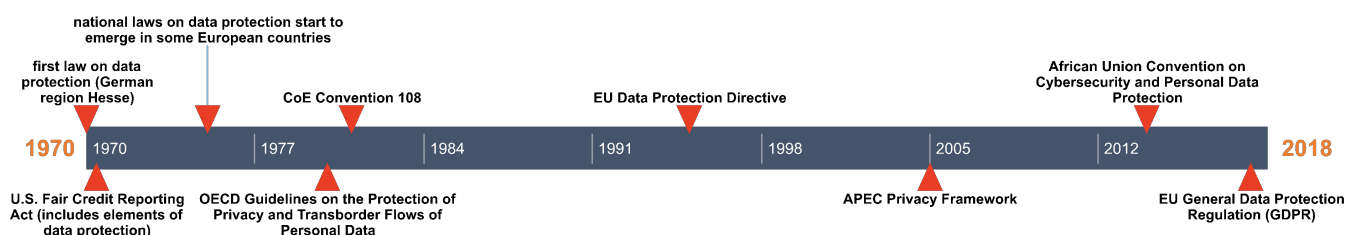


## 5. Legal Frameworks in TIP Data Collection

Laws 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 rights of data subjects – are to be protected.<sup>76</sup> Important questions arise concerning who owns data when it is collected and who has the right to access, change, delete and disseminate it.

In answer to these questions, **data protection principles** emerged and were eventually articulated and codified in data protection laws and regulations. The first law on data protection was passed in 1970 in the German region of Hesse.<sup>77</sup> Around the same time, some elements of data protection were addressed in the U.S. *Fair Credit Reporting Act* of 1970 and fair information practices were developed in the U.S. in the early 1970s.<sup>78</sup> Awareness of potential threats to data simultaneously emerged in the UK and national laws were enacted in some countries in Europe (Sweden, Germany and France) as well as in the U.S.

### *Timeline #1. Development of legal frameworks for data protection*



In the following decade, the Organization for Economic Cooperation and Development (OECD) developed privacy principles in its 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, shortly before the Council of Europe's 1981 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (CoE Convention 108) came into force.<sup>79</sup> CoE Convention 108 is a comprehensive international data protection law; it has the force of law for states parties to it and is open to non-European signatories.<sup>80</sup>

The *EU General Data Protection Regulation* (GDPR), which entered into force in May 2018, represents the most robust regional instrument on data protection to date.<sup>81</sup> In light of the

<sup>76</sup> See Privacy International (2017) *Privacy International*.

<sup>77</sup> State of Hesse (1970) *Datenschutzgesetz* [Data Protection Act] of October 7, 1970, Hessisches Gesetz-und Verordnungsblatt I.

<sup>78</sup> Government of the United States (1970) *Fair Credit Reporting Act*, 15 U.S.C. § 1681. Washington, D.C., United States: U.S. Government.

<sup>79</sup> CoE (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108. Strasbourg, France: Council of Europe.

<sup>80</sup> As of January 2018, CoE Convention 108 has been ratified by 51 states (including 4 non-members of the Council of Europe: Mauritius, Senegal, Tunisia and Uruguay).

<sup>81</sup> EUGDPR (2018) *EU General Data Protection Regulation Portal*. See Section 5.3 on regional legal frameworks for an in-depth discussion of the GDPR.



cross-border nature of data processing,<sup>82</sup> this instrument has far-reaching ramifications extending beyond Europe and will likely impact how legislative frameworks for protection around the world are subsequently developed.

Considerations of legal issues and relevant legal frameworks for TIP data collection are relatively new and quickly changing, particularly as new challenges emerge in light of increased cross-border data processing, rapidly advancing informational 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. The relevant legal frameworks for TIP data collection 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. For example, financial privacy laws may have significant bearing on data collection vis-à-vis money laundering and financial aspects of crimes committed by suspected traffickers, as one NGO director noted:

When we talk about financial information, we have to relate that to whether or not there's a banking secrecy issue there.

Similarly, health privacy laws (a specific category of privacy law) may have bearing on health-related data collected by service providers working with trafficking victims as part of case management.

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;<sup>83</sup>
- **Criminal justice laws**, that may be relevant to the protection of suspected perpetrators and presumed or identified victims of crime;
- **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).<sup>84</sup>

---

<sup>82</sup> Data processing is when data is processed or organized for analysis.

<sup>83</sup> For example, *The International Compilation of Human Research Standards* (formerly known as the *International Compilation of Human Subject Protections*) enumerates over 1,000 laws, regulations and guidelines that govern human subjects research in 103 countries, as well as the standards from a number of international and regional organizations. This Compilation was developed for use by researchers, IRBs/Research Ethics Committees, sponsors and others who are involved in human subjects research around the world. HHS (2017) *International Compilation of Human Research Standards*. United States: Office for Human Research Protections, U.S. Department of Health and Human Services.

<sup>84</sup> United Nations (2015) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, UN Doc A/HRC/29/32.

Which categories of law (and, within them, which provisions) will be relevant to TIP-related data collection will vary significantly depending on the overall purpose of data collection, the person or entity collecting data, the participants from whom data is collected and the nature of the data. Identifying the relevant law (or laws) can be a complicated determination. As one NGO director noted:

You've got to sit down and determine in each different case what are the relevant sensitivities, what are the rights, what are the obligations, what are you planning to do with the information? And is what you're planning to do within the scope of the restrictions that are set out by law? Do you have the right to do this? Have you sought consent? Do you need to seek consent? Are you obligated to behave in a certain way, are certain circumstances triggered by certain information?... Those should be the first steps of analyzing whether information can be used for whatever is [needed]. And, in cases of protection, it has got to be big issues like safety of the individual, safety of those around them and in relation to legal privilege, in relation to medical information, financial information.

It is not always feasible for data collectors working on TIP data collection projects to parse the complex body of laws related to data collection within their current efforts and resources. This requires legal expertise and knowledge of the legalities around data. One NGO director noted the inexperience of many NGOs in appreciating the legalities surrounding data collection:

You'll find NGO staff are very unused to the rigor around data collection and holding data. And also, the fact that it's not theirs, it's the data of the victim and regardless of how traumatized the victim is, the truth is that they should give express consent.

In this vein, what **data ownership** means for individuals (for example, trafficking victims) merits discussion. Data firstly 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. For example, according to Article 12 of the 1995 EU *Data Protection Directive*, individuals have the right to obtain information as to whether or not their personal data is being processed, the purpose of such processing, the source and content of the data concerned, and to whom the data is disclosed.<sup>85</sup> Article 15 of the 2018 EU *General Data Protection Regulation* (GDPR) ensures this same right.<sup>86</sup> In addition, individuals have the **right to object** at any time to the processing of data relating to them.<sup>87</sup>

However, in practice, it is not always feasible to exercise one's data ownership rights. As noted in one study on data protection in the EU, these rights – to access, correct, object – are expressed in general terms and without details about how an individual can exercise these rights. There are also no deadlines set for responding to requests from data subjects or guidelines for fees that may be requested relating to the rectification, erasure and blocking of personal data.<sup>88</sup>

---

<sup>85</sup> EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union, Article 12. The same Article establishes that individuals have the right to correct, erase, or block the transfer of inaccurate or incomplete data. It is also required that individuals can exercise privacy rights in an easy manner without constraints, at reasonable intervals of time, and without excessive delays or expenses.

<sup>86</sup> EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union ("General Data Protection Regulation" or GDPR).

<sup>87</sup> EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union, Article 14.

<sup>88</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p. 30. The data subject's rights may be exempted or restricted under certain circumstances,

In real terms, then, 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. They may be unaware of how the data is analyzed and not be informed of any changes to its use, let alone be 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.<sup>89</sup> More generally there is a disconnect between what protections laws afford and how these protections work in practice.

**Box #6. Navigating the legal framework related to privacy in implementing anti-trafficking projects<sup>90</sup>**

From 2008 to 2012, the Netherlands Ministry of Justice launched eight anti-trafficking pilot projects to promote cooperation between investigative agencies and to test and generate insights into what information might be relevant to share. Analysis of the pilot projects showed time, experience and trust were important factors in how long it took before information sharing commenced. One pilot project took more than a year to create a legal framework for information-sharing between the various project partners, primarily because each organization was bound by a different interpretation of privacy legislation, which, in turn, impacted how information was managed and used.

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, data collectors may find it 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

collectors should identify and comply with the highest standards.

An example from the Netherlands in Box #6 above illustrates the difficulty in navigating the legal framework related to privacy in the implementation of anti-trafficking projects. More specifically, the time needed to analyze the legal framework for information exchange between state institutions was a set-back for this project, as the former Dutch National Rapporteur described (of these pilot projects in the Netherlands):

The greatest challenge proved to be creating the legal framework required in connection with privacy legislation. In every pilot, the legal framework was laid [out at the start of the project] ... Nevertheless, the complexity of the applicable legislation as well as caution on the part of some [pilot project] partners, caused some delay in advancing the exchange of information. The reluctance appears to have been due mainly to ignorance of what the law did or did not allow in terms of sharing information or to a lack of trust in other chain partners.<sup>91</sup>

---

including to safeguard national security, national defense, public security, the prosecution of criminal offences, an important economic or financial interest of a member state or of the European Union, or for the protection of the data subject or the rights and freedoms of others.

<sup>89</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment*. Responsible Data Forum.

<sup>90</sup> Dutch National Rapporteur (2013) *Trafficking in Human Beings. Ninth report of the Dutch National Rapporteur*. The Hague, Netherlands: Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children, p. 271.

<sup>91</sup> Dutch National Rapporteur (2013) *Trafficking in Human Beings. Ninth report of the Dutch National Rapporteur*. The Hague, Netherlands: Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children, pp. 272-272.

One study in the EU highlights the need for clearly defined roles and obligations in relation to data protection for NGOs providing services to trafficking victims, noting that current legal instruments are not always clear:

International, regional, and national political and legal instruments contain only vague descriptions on the structure and role of civil society cooperation with authorities regarding data collection and data protection. For this reason, it is important that future guidelines advising NGOs on their role as data processors be elaborated and that their role is clarified in national and international data collection tools, such as the National Rapporteur and/or equivalent mechanisms. The 2011 [EU *Trafficking Directive*] recommends that civil society stakeholders seek cooperation with National Rapporteur Mechanisms but fails to define the role and mandate of NGOs in this context.<sup>92</sup>

This is pressing given that, in some countries, some responsibilities, like assisting trafficking victims, are generally undertaken by NGOs, which may result in rights or legal obligations to share data collected in the context of their daily work with the government. This is particularly complex when these NGOs (and the services they provide) are funded by the state as the possibility could arise for the government to demand access to or even ownership of the data collected. Access and perhaps ownership issues may still arise when the state is not funding the NGO or its services.

In the United States, the applicable data protection laws may be linked to funding for anti-trafficking service providers. For example, helplines or service providers that receive funding under the *Violence Against Women Act* (VAWA) are subject to VAWA restrictions on data collection and sharing. VAWA does not prohibit the collection of personal data by service providers but does prohibit sharing personally identifying information about victims without informed, written and reasonably time-limited consent. These confidentiality grant conditions also prohibit programs from making the signing of a release (where an individual receiving services consents to have their information collected and shared) a condition of service. VAWA further states that grantees may not “disclose, reveal or release any personally identifying information or individual information collected in connection with services requested, utilized, or denied through grantees’ and sub-grantees’ programs, regardless of whether the information has been encoded, encrypted, hashed, or otherwise protected”.<sup>93</sup>

There are also issues around data sharing within an organization and between organizations. For example, data sharing might involve a person from NGO(a) sharing data with another person in that same NGO, or, in some cases, with someone from NGO(b) in a neighboring town, or even with someone in NGO(c) in another country. When sharing data externally (for instance, when one NGO shares data with another NGO) a degree of control can be maintained by limiting what is shared and how it is shared.<sup>94</sup> Indeed whether and how data is shared may be mandatory or optional, depending on the source of funding, the nature of the organization, legal obligations, victim consent and so on. These must be weighed against both the benefits and risks of sharing data, particularly for data subjects.

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

---

<sup>92</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p. 76.

<sup>93</sup> Government of the United States (2013) *Violence Against Women Reauthorization Act*, 42 USC §13925(b) as amended. Washington, D.C., United States: U.S. Government.

<sup>94</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Department*. Responsible Data Forum, pp. 84-85.

regulatory frameworks. Multi-jurisdictional contexts are a growing 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 very often a lack of legislative certainty on data ownership and responsibilities.<sup>95</sup> This is further complicated by online activities (like social networking sites and cloud computing) and the fact that collecting personal data has become increasingly sophisticated and less easily detectable.<sup>96</sup> 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. National legislation concerning Intellectual Property (that is, database rights, copyright, trade secrets) may indirectly come into play, but often these laws are essentially silent on questions of who owns the data. Such legislation does impact on data sharing obligations depending on factors such as the sector concerned and the public interests served, whether for public health or public security purposes, for instance.<sup>97</sup>

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 discuss these various frameworks.



## 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.<sup>98</sup> Data protection (privacy) legislation varies widely across countries. Many countries in North and South America, Europe and Asia<sup>99</sup> have explicit laws on data protection and privacy. For example, all EU member states have transposed the 1995 *Data Protection Directive* and are upgrading their legislation in line with the *General Data Protection Regulation (GDPR)*.<sup>100</sup> By contrast, specific data protection laws in countries in South Asia, sub-Saharan Africa and the Middle East are largely lacking.<sup>101</sup> However, many countries in these regions are currently working to amend their legislation in line with new risks posed by information communications technologies and to bring their approaches in line with regional and

---

<sup>95</sup> For example, according to the European Commission, it is not always clear to either data controllers or data protection authorities (DPAs) which member state is responsible and/or which laws are applicable when several member states are involved. There is also confusion when a multi-national organization is established in different member states or when the data controller is not established in the EU but provides services to EU residents. EC (2010) *Communication on a Comprehensive Strategy on Data Protection in the European Union*. Brussels, Belgium: European Commission.

<sup>96</sup> EC (2010) *Communication on a Comprehensive Strategy on Data Protection in the European Union*. Brussels, Belgium: European Commission.

<sup>97</sup> César, J., J. Debussche and B. Van Asbroeck (2017) 'White Paper - Data ownership in the context of the European data economy: Proposal for a new right', *Bird & Bird*.

<sup>98</sup> Smith, B. (2018) 'A problem Congress should solve', *Microsoft On the Issues*, February 27.

<sup>99</sup> For instance, Singapore, Malaysia and the Philippines have dedicated data protection laws; in Indonesia, Myanmar and Vietnam data privacy requirements are part of electronic transaction laws. For more, see Chow, K.W. and N. Redfearn (2016) 'Data protection in ASEAN', *Rouse*.

<sup>100</sup> See Section 5.3 on regional legal frameworks for an in-depth discussion of the GDPR.

<sup>101</sup> For example, there are no data protection laws for the private sector in Pakistan, Bangladesh, Sri Lanka, Nepal, the Maldives, Bhutan and Afghanistan, although there is data privacy regime in Nepal's public sector; a *Right to Information (RTI) Act* with some data privacy extensions in Bangladesh; computer crime and compensation provisions in Sri Lanka, Bangladesh and Pakistan; and constitutional protections in most of these countries. Greenleaf, G. (2014) *Privacy in the Other Seven South Asian (SAARC) States*. Oxford, United Kingdom: Oxford University Press.

international standards for data protection.<sup>102</sup> Whether data protection and privacy violations are addressed by provisions in administrative law, criminal law or a combination of both varies from country to country.

Where there is legislation in place, there is notable overlap between the principles captured therein, largely because much legislation is based on common frameworks, including the EU *General Data Protection Regulation (GDPR)* as well as the Organization for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC) *Privacy Frameworks*, which offer a source of principles and regulations governing data protection that are to be implemented at the level of national legislation.<sup>103</sup> 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 (that is, 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.

In some jurisdictions, depending on how the laws are drafted, data and privacy considerations may be addressed by the same act. For instance, "The Data Protection (Privacy) Act" or the "Privacy (Data Protection) Act" in a given country may be a privacy law containing a subsection about the use, collection, and so on of data. That subsection on data protection can be further subdivided in many ways (for example, by type of data, by public and private organizations or by specific topics as it evolves to address new things like telecommunications and Big Data). In some countries, a constitution or bill of rights may set out the broader privacy rights of individuals and the specifics of data protection could be dealt with in a separate legal act or acts that are informed by (and must be interpreted in accordance with) that constitution or bill of rights. In still other cases, there may be no specific data protection law but rather specific provisions of relevance may be captured within criminal codes or tort law.

As data is increasingly collected across multiple jurisdictions, lack of legislative harmonization may result in gaps in protection for data subjects. For instance, the U.S. takes a more permissive, sectoral-based approach than is provided for by the more protective and overarching EU legislation.<sup>104</sup> The U.S. *Privacy Act* of 1974 applies only to the Federal Government and only protects U.S. citizens and residents.<sup>105</sup> The U.S. *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) regulations, while comprehensive, only protect the privacy and security of certain health information. Meanwhile, a detailed and

---

<sup>102</sup> For example, Qatar passed a law on data protection in November 2016. Government of Qatar (2016) *Law No. 13 Concerning Personal Data Protection (the Data Protection Law)*. Qatar: Government of Qatar.

<sup>103</sup> See Section 5.3 on regional legal frameworks for an in-depth discussion of the GDPR, OECD and APEC *Privacy Frameworks*.

<sup>104</sup> Schriver, R.R. (2002) You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission', *Fordham Law Review*, 70(6).

<sup>105</sup> Privacy International (2017) *Privacy International*.

comprehensive approach is taken in the EU, imposing obligations on a wider range of actors. The GDPR for implementation across EU member states, applies to EU individuals, organizations and companies that are either controllers or processors of personal data.<sup>106</sup> The GDPR applies to data processed about persons in the EU, including where processes are located beyond the borders of the EU. And it applies protection to all natural persons, whatever their nationality or place of residence, meaning that foreign victims of trafficking who are in the EU – even those in irregular situations – are protected.<sup>107</sup>

While it is impossible to accurately generalize about 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. Key issues include: scope and applicability, definitions, guiding principles and compliance.

#### National Legal Frameworks

- Scope and applicability
- Definitions
- Guiding principles
- Compliance

### 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.<sup>108</sup> According to an Organization of American States (OAS) study, legislation on personal data protection takes one of three approaches:

- 1) the European system is the strictest with legislation governing both data collection by governments and private organizations;
- 2) U.S. legislation, which guards against government intrusion only, leaving private industries to self-regulate; and
- 3) the Latin American system, which is based on the concept of *Habeas Data*, a constitutional right allowing individuals to access their personal data, issue complaints and correct data that may have injured their right to privacy.<sup>109</sup>

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.

---

<sup>106</sup> EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union (“General Data Protection Regulation” or “GDPR”). For a detailed discussion of the EU legal framework for data protection, please see Section 6.1.3.

<sup>107</sup> EU General Data Protection Regulation 2016/679, Article 14.

<sup>108</sup> Personal/domestic purposes refers to the collection and use of data for an individual’s personal, family or household affairs (including recreational purposes). Examples include maintaining an address book of friends and acquaintances on a personal device; keeping files related to personal commercial affairs such as bank statements; holding the health records of family members and so on. However, as information and communications technology (ICT) has developed a range of personal processing activities not foreseen in many existing privacy laws, legal uncertainty may exist in terms of the scope and applicability of privacy/data protection laws. For example, does an individual posting personal data openly for a worldwide unrestricted audience on the internet still fall under the exception of processing data for personal or household purposes? See EU (2013) *Annex 2: Proposals for Amendments regarding exemption for personal or household activities*. Brussels, Belgium: European Union.

<sup>109</sup> OAS (2011) *Draft: Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data)*, Document presented pursuant to General Assembly Resolution AG/RES.2514. Washington, D.C.. United States: Organization of American States.

## Definitions

National laws generally offer a definition of both personal data (or 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 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. Collection of sensitive data is severely restricted, except in exceptional circumstances and often with specified conditions. Terms such as **data owner** are used to refer to the data subject and **data controller** is taken to apply to the person who has collected and processed the data.

## 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, the right to correct data, the right to rectify, erase or block data and the right to object and complain. Sometimes these rights are limited only to citizens or permanent residents, potentially raising gaps for trafficked persons or perpetrators of trafficking in irregular situations.<sup>110</sup> The obligations of data controllers include the obligation to seek consent, to inform data subjects and regulatory bodies or government ministers of key events (such as a security breach resulting in unauthorized access to personal data), to process data anonymously and maintain confidentiality even after the relationship between the controller and their employer or with the data subject has ended.

While these rights and obligations may feature in several national data protection instruments, the ways that they are interpreted in practice may differ significantly. For instance, what constitutes valid consent and how coercion is understood may differ between jurisdictions.<sup>111</sup> In relation to informing data subjects, the information they must be informed about, when and through what mediums may differ. Similarly, the standards of anonymity and confidentiality may differ, in terms of time frames for when the relationship between data subjects and data controllers is considered to have come to a close and what actions must be taken when it does.

Guiding principles capture rights and obligations in legislation and are generally similar across countries. While they are captured in different orders and grouped together in different ways, they generally include principles such as:

- Collection of data only for a specified use and in accordance with law;
- Non-processing of data beyond that purpose;
- Not keeping data longer than necessary to the purpose;
- Accuracy of data and keeping it up to date;
- Taking appropriate technical and organization measures to secure data against unlawful processing, accidental loss, damage or destruction;

---

<sup>110</sup> This is not the case for the EU GDPR, which applies to protection of all natural persons, whatever their nationality or place of residence (domestic laws implemented in accordance with the GDPR would follow suit). EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union ("General Data Protection Regulation").

<sup>111</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., 25-27



- Not transferring data outside the country or territory except where the recipient country or territory ensures adequate or equivalent protection of the rights of data subjects in relation to processing of data.

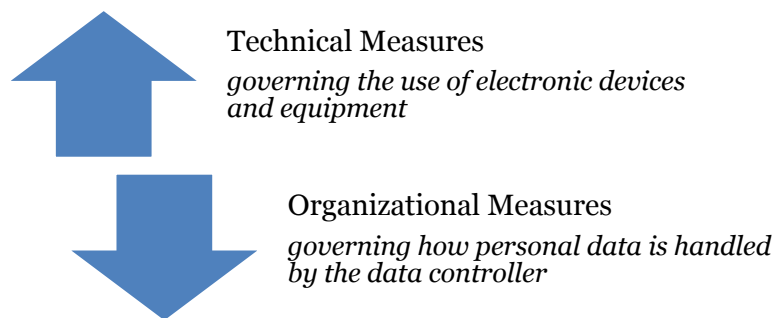
How these principles are interpreted and applied in practice differ between and indeed within countries.

## 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.<sup>112</sup>

Diagram #2. Categories of security measures to protect data



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.

Sanctions for non-compliance can range from financial liability for damages or involve administrative or criminal sanctions, to, at the most extreme, imprisonment for severe violations of privacy. As one criminal justice expert noted:

I was working with prosecutors and investigators and they made it clear to me that they could not actually show me the files or provide me with details of the investigation unless I were to sign an agreement that should I then disclose that information outside the criminal justice arena (in any kind of report or publication or even verbally, outside the criminal justice system of that country) that I would be subject to their criminal procedures. That could make me liable, put me in jail for violating their privacy act.

As with all national legislation, whether it relates to data protection generally, trafficking in persons specifically or other fields entirely, effectiveness depends on implementation in

<sup>112</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin: KOK e.V., p.27

practice. The creation of independent supervisory or regulating bodies with authority to monitor data processing is a significant step towards strengthening data protection implementation and one that is being taken in an increasing number of countries.

Reviewing the national legal framework for the country/countries where TIP data collection takes place is an essential starting point and relevant resources on national laws are outlined in Table #2: *Resources on national laws relevant to data protection*, below.

Table #2. *Resources on national laws relevant to data protection*

<b>Resources on national laws relevant to data protection</b>	
BakerHostetler (2015) <i>International Compendium of Data Privacy Laws</i> . United States: BakerHostetler.	A resource on data privacy laws in several countries around the world.
Bali Process (2015) <i>Privacy and data protection laws of Bali process member states</i> . Bali: Bali Process.	This document analyzes privacy and data protection laws of Bali process member states, with a view to strengthening data protection in the context of human trafficking
DLA Piper (2017) <i>Data Protection Laws of the World Handbook</i> . London: DLA Piper.	A resource primarily for corporate actors to understand privacy legislation; of value for anti-trafficking stakeholders.
HHS (2017) <i>International Compilation of Human Research Standards</i> . United States: Office for Human Research Protections, Department of Health and Human Services.	A two-volume collection of laws on human subjects research standards and laws, including data and privacy laws.
UNCTAD (2016) <i>Data Protection Regulations and International Data Flows: Implications for Trade and Development</i> . Geneva: United Nations Conference on Trade and Development.	A collection of essays on data protection laws of select countries.
ZICO Law (2016) <i>ASEAN Insiders: Personal Data Protection</i> . ZICO Law.	A brief overview of the data protection laws in Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Singapore, Thailand and Vietnam.

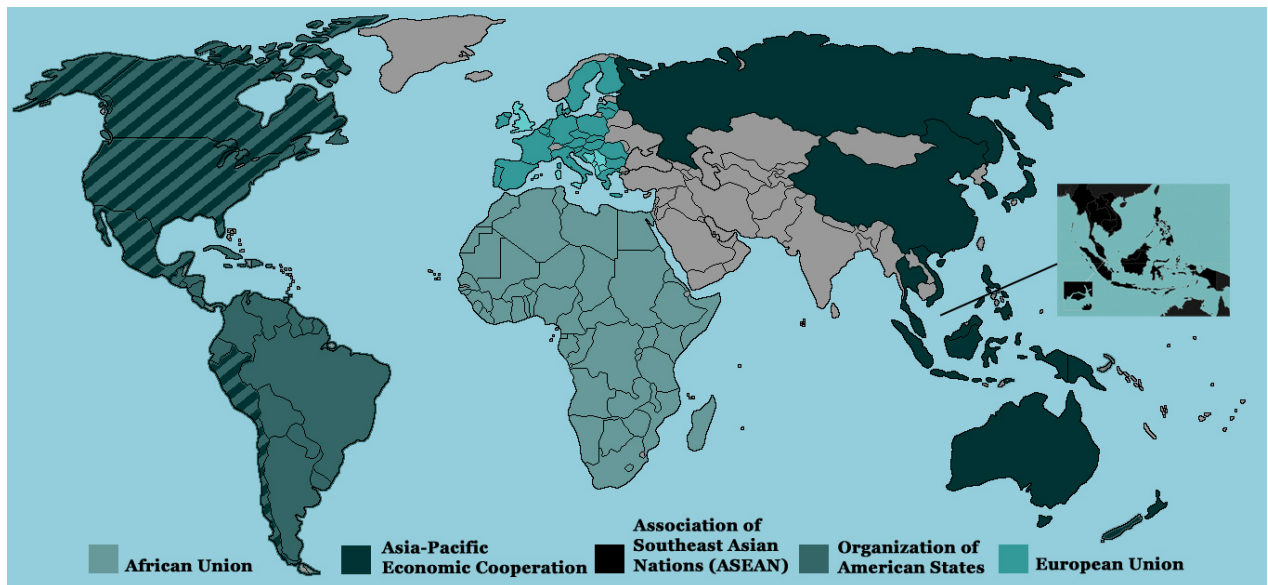


### 5.3 Regional legal frameworks

Different regions are at very different stages in the development of legislative and policy infrastructures for data protection. Some regional legislative frameworks are comprehensive. 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. In other regions, legislation is entirely lacking.<sup>113</sup> Moreover, even when regional frameworks do exist, questions around implementation persist.

<sup>113</sup> For example, there are no harmonized laws or policies on data protection across the GCC (Gulf Cooperation Council) region or via the Organization of Islamic Cooperation, although some individual countries are taking steps to introduce national laws on data protection.

Map #2. Regions with legal frameworks relevant to TIP data collection



### 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, as detailed in Table #3 below.

### European Union Legal Framework

- Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Data (1981)
- 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)
- 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 Data Protection Directive 95/46/EC (1995)
- European Union Directive 2016/680 on data protection in the area of police and justice (2016)
- Council of Europe Convention on Action against Trafficking in Human Beings (2005)
- 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 European Convention on Human Rights (1950)
- European Union Charter of Fundamental Rights (2000)

### **Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Data (1981) (COE Convention 108)**

CoE *Convention 108* remains the main instrument governing the processing of domestic data in criminal matters in the European Union.<sup>114</sup> The importance of the Convention and the adoption of legal rules in accordance with it is especially important in light of increased use of computers and the internet and the resultant rise of high speed data transactions.<sup>115</sup> The Convention protects against privacy intrusions by public and private authorities whether offline or online.<sup>116</sup>

CoE *Convention 108* remains important and relevant because it provides guarantees on personal data processing and prohibits processing of sensitive data in the absence of legal safeguards. It also protects the right of the individual to know that information is stored on them and to have it corrected if necessary. CoE *Convention 108* restricts cross-border flows of personal data to states where legal regulations provide inadequate protection.<sup>117</sup> CoE *Convention 108* also applies to activities in the areas of national security and law enforcement, covering data protection across all areas of policing.<sup>118</sup>

By virtue of Article 10, member states are required to enact CoE *Convention 108* into domestic law and establish appropriate sanctions and remedies for violations of its principles. Sanctions and remedies may be civil, administrative or criminal depending on the situation in a given state. CoE *Convention 108* provides for several exceptions that may be relevant for TIP-related data, including, for instance, where necessary for suppressing criminal offences.<sup>119</sup>

The Explanatory Note to the CoE *Convention 108* offers insight into automatic data collection and storage challenges and corresponding protection obligation of the data collectors/users:

“Information power” brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerized data files: payroll, social security records, medical files, etc. It is essential that those responsible for these files

---

<sup>114</sup> As of December 2018, CoE *Convention 108* has been ratified/acceded by 53 states (including 4 non-members of the Council of Europe: Mauritius, Senegal, Tunisia and Uruguay).

<sup>115</sup> See EPIC (2017) *Electronic Privacy Information Centre* and FRA (2014) *Handbook on European Data Protection Law*. Vienna, Austria: European Union Agency for Fundamental Rights, pp.15-17.

<sup>116</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p.45.

<sup>117</sup> A separate Framework Decision was adopted in 2008 (Framework Decision 2008/977/HA) pertaining to cross-border data processing. Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., pp. 19-20. See also FRA (2014) *Handbook on European Data Protection Law*. Vienna, Austria: European Union Agency for Fundamental Rights, pp.15-17 and EDPS (2012) *Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – ‘The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016’*. Brussels, Belgium: European Data Protection Supervisor, p. 2. The European Data Protection Supervisor (EDPS) is a supervisory authority established to protect personal data and privacy and implement best practices within the EU. Regarding the protection of human trafficking data, the EDPS emphasizes the role of data protection as a pre-condition to relationships of trust between stakeholders and as a part of victim’s rights including the right to information. The EDPS further emphasizes the role of data protection in the EU-wide data collection system and in the context of rights-based anti-trafficking policies and other measures.

<sup>118</sup> See also CoE (1987), *Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector*. Strasbourg, France: Council of Europe Committee of Ministers, which sets out how data should be collected, kept, accessed, transferred, secured and how data subjects should be able to exercise their data protection rights.

<sup>119</sup> These derogations are in relation to the quality of data (Article 5), sensitive data (Article 6) and additional safeguards for data subjects (Article 8), where such derogations are necessary on particular grounds including for the suppression of criminal offences (Article 9(2)). CoE (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108. Strasbourg, France: Council of Europe.

should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored. For this reason, they should maintain the good quality of the information in their care, refrain from storing information which is not necessary for the given purpose, guard against unauthorized disclosure or misuse of the information and protect the data, hardware and software against physical hazards.<sup>120</sup>

In the 40 years that have passed since this explanatory note was drafted, the technological capacity for automated data collection and storage has increased dramatically. Responding to evolutions in technology, recent case law on data protection and data privacy violations in the EU has underlined the need to strengthen CoE *Convention 108* in the protection of individuals in light of technological developments.<sup>121</sup> Accordingly, the Council of Europe is modernizing CoE *Convention 108*, notably to ensure accountability of data processors and processes, strengthen the obligation to declare data breaches, ensure transparency of data processing and add safeguards for the data subject, including through the right to obtain knowledge of the logic underlying data processing and to object.<sup>122</sup>

Also of relevance in understanding CoE *Convention 108*, is the CoE Committee of Ministers *Recommendation (87)15 to member states regulating the automated processing of personal data in the police sector* (CoE *Police Recommendation*). The CoE *Police Recommendation* refers to the *Convention for the Protection of Fundamental Rights and Human Freedoms*, asserting eight principles for police to follow regarding data collection and protection. These principles mirror data protection principles found in other contexts, including control and notification, collection of data, storage, use and its limitation, communication and safeguards thereto, right of access and rectification, limited storage time and data security.<sup>123</sup>

### **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)**

In 2016, the *General Data Protection Regulation* (GDPR) repealed the 1995 EU *Data Protection Directive* (discussed below).<sup>124</sup> The GDPR replicates components of the *Data Protection Directive* and also enhances it, giving explicit consideration to electronic means of data processing in light of technological developments and extending its scope to include law enforcement agencies, which were not covered by the *Data Protection Directive*. The GDPR aims to simplify and harmonize data protection across EU member states as well as ensure a single supervisory decision in cross-border cases where several national data protection authorities are involved.<sup>125</sup> The deadline for the GDPR to be implemented across all EU member states was May 2018.

---

<sup>120</sup> CoE (1981) *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Explanatory Report*. Strasbourg, France: Council of Europe.

<sup>121</sup> See, for instance, *Maximillian Schrems v Data Protection Commissioner* (2015) Judgment in Case C-362/14 (concerning data privacy violations by Facebook); *Szabo v Hungary* (2016) European Court of Human Rights No. 37138/14 (concerning anti-terrorist surveillance without sufficient safeguards against abuse); and *Zakharov v Russia* (2015) European Court of Human Rights No. 47143/06 (concerning surveillance of mobile phone communications in Russia).

<sup>122</sup> CoE (2017) ‘Modernization of the Data Protection Convention 108’, *Council of Europe*, January 28.

<sup>123</sup> See also CoE (1987), *Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector*. Strasbourg, France: Council of Europe Committee of Ministers, which sets out how data should be collected, kept, accessed, transferred, secured and how data subjects should be able to exercise their data protection rights.

<sup>124</sup> EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union.

<sup>125</sup> UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, p. 32.

The GDPR applies extraterritorially if a data controller or processor or a data subject is based in the EU. Significantly, the regulation will also apply to processors based outside of the EU if they process any personal data from within the EU. In practice, this means that a website outside of the EU that is accessed by people within the EU may be subject to the GDPR if it collects personal data, the definition of which the GDPR has broadened to include IP<sup>126</sup> and email addresses. Accordingly, the GDPR will have significant impact in Africa, Asia, the United States and elsewhere as data protectors and controllers outside of Europe process data of individuals who are located within the EU and are consequently required to have GDPR-compliant data protections in place. It is likely that jurisdictions outside the EU will be required to take steps to bring their frameworks into compliance with the higher standards provided for in the GDPR.

According to Article 4(1) of the GDPR, **personal data** means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. As such, what can be considered to be personal data is very broadly understood. According to the European Commission:

Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the internet.<sup>127</sup>

The GDPR imposed several important practical requirements. For example, organizations whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale (or special categories of data or data relating to criminal convictions and offences) must appoint a Data Protection Officer, who is an expert on data protection law and practice. The GDPR also introduces administrative requirements, including keeping written records of data processing activities and carrying out data protection impact assessments.

Another key aspect of the GDPR is that it strengthens the right of **data erasure** or the “right to be forgotten”. Article 17(1) sets out that the data subject has the right to obtain from the controller the erasure of personal data concerning the data subject without undue delay, and that the data controller has the obligation to erase personal data without undue delay, where one of several listed grounds applies, including (among others) the fact that the data are no longer necessary, consent is withdrawn or the data have been unlawfully processed.

### **European Union Data Protection Directive 95/46/EC (1995)**

The 1995 EU *Data Protection Directive*<sup>128</sup> was the primary instrument on data protection in European Union law until the GDPR came into effect in May 2018 and continues to have significant influence on global policy developments on data protection.<sup>129</sup> All EU states have

---

<sup>126</sup> An Internet Protocol (IP) address is a unique numeric label that identifies an individual computer using the Internet.

<sup>127</sup> EC (2012) ‘Commission proposes a comprehensive reform of data protection rules to increase users’ control of their data and to cut costs for businesses’, *European Commission Press Release Database*, January 25.

<sup>128</sup> EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union.

<sup>129</sup> UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, p. 32.

brought their legislation into line with the EU *Data Protection Directive*, as have many neighboring states and countries wishing to join the EU. As the GDPR replicates components of the *Data Protection Directive*, the *Data Protection Directive* is still a critical part of the legal framework for data protection in the European Union. The definitions and principles contained therein are the main reference for data provisions in other instruments, not only within, but also beyond the EU. For example, **sensitive data** is defined by Article 8(1) as: “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life”. Processing of sensitive data is prohibited as a general rule, with some limited exceptions specified. Whether data pertaining to human trafficking is sensitive data is an important question, particularly in relation to victims and perpetrators of trafficking crimes.<sup>130</sup>

The 1995 EU *Data Protection Directive* requires EU member states to enact laws to govern the processing of personal data according to specified minimum standards. However, as noted above, it does not apply to data processing activities in the area of police and judicial cooperation in criminal matters.<sup>131</sup> Accordingly, the *Data Protection Directive* applies to the collection of some human trafficking related data, but not to all, depending on the context. There are seven principles grounding the *Data Protection Directive*, pertaining to the purpose of data use, consent, security of data, information about data and disclosure.<sup>132</sup> On the basis of those principles, it is clear that personal data should not be used without knowledge or unambiguous informed consent of the data subject. Further, data should be correct, relevant and not excessive in relation to the purpose for which it is stored. The use of data, including its disclosure, should be carried out accurately.<sup>133</sup>

### **European Union Directive 2016/680 (“Data Protection Directive for the Police and Criminal Justice Sector”) (2016)**

The EU legal framework also provides for data protection across police work with principles comparable to those specified in the GDPR.<sup>134</sup> This framework is relevant to TIP criminal

---

<sup>130</sup> For example, data collected about a victim of trafficking for the purpose of sexual exploitation may be considered an intimate part of a person’s privacy and, accordingly, only permissibly collected for the most limited reasons. Or in some countries where sex work/prostitution is recognized as a form of work, it may not be considered as part of a person’s “sex life”. Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p.39. The European Court of Human Rights interprets “private life” broadly to afford the widest possible protection, without distinguishing between private and professional life in doing so. See *Niemietz v. Germany* (1992) European Court of Human Rights, 16 December 1992, Application No. 13710/88, § 29; *Schecke & Eifert* (2010) European Court of Justice, 9 November 2010, C-92/09 and C93/09, § 59; and *Österreichischer Rundfunk and Others* (2007) European Court of Justice, 8 November 2007, C-456/00, §73, referred to in Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., pp.39-40.

<sup>131</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., p.19.

<sup>132</sup> The principles for the protection of personal data include: notice (data subjects should be given notice when their data is being collected); purpose (data should only be used for the purpose stated and not for any other purposes); consent (data should not be disclosed without the data subject’s consent); security (collected data should be kept secure from any potential abuses); disclosure (data subjects should be informed as to who is collecting their data); access (data subjects should be allowed to access their data and make corrections to any inaccurate data); and accountability (data subjects should have a method available to them to hold data collectors accountable for not following the above principles).

<sup>133</sup> Roth, P. et al. (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V., pp. 21-22.

<sup>134</sup> EU (2016) *Directive 2016/680 on the protection of data of natural persons with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data*. Brussels, Belgium: European Union (“Data Protection Directive for the Police and Criminal Justice Sector”). The European Court of Human Rights has considered data retention by police or national security authorities in several occasions. *Allan v. the United Kingdom* (2002) European Court of Human Rights, 5 November 2002, No. 48539/99; *B.B. v. France* (2009) European Court of Human Rights, 17 December 2009, No. 5335/06; *Leander v. Sweden* (1987) European Court of Human Rights, 26 March 1987, No. 9248/81; *M.K. v. France* (2013) European Court of Human Rights, 18 April 2013, No. 19522/09; *M.M. v. the United Kingdom* (2012) European Court of Human Rights, 13 November 2012, No. 24029/07; and *S. and Marper v. the United Kingdom* (2008) European

justice data collection. The *Data Protection Directive for the Police and Criminal Justice Sector*, adopted in (and applicable as of) May of 2016,<sup>135</sup> harmonizes the legal framework surrounding protection of personal data and its flow between authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences within the EU, as well as the transfer of that data to countries outside of the EU and to international organizations that are deemed competent authorities for criminal justice purposes. Prior to the adoption of the Directive, such data was protected in different ways depending on which authority had competence in relation to the data.

While many principles of the *Data Protection Directive for the Police and Criminal Justice Sector* are the same as those provided in the GDPR, the Directive does not provide the same high level of rights for data subjects as is the case with the GDPR, for the practical reason that it attempts to balance the rights of human subjects with criminal justice objectives. That is, allowing traffickers rights to access their personal data could hamper investigations. Nonetheless, the Directive provides rights to data subjects, establishes obligations of data controllers and processes and prescribes technical measures to ensure the security of personal data including in the transfer of that data to third countries or international organizations.

The Directive does not apply to processing of personal data in the course of an activity that falls outside of the scope of EU law. It is unclear what the ramifications would be, for example, in the transfer of personal data in trafficking investigations to third countries that define the crime of trafficking differently (or not at all). As a Directive rather than a Regulation, States have a certain degree of flexibility in terms of how they interpret its provisions and incorporate them into national laws.<sup>136</sup>

### Other relevant EU instruments

In addition to the data protection instruments mentioned above, there are provisions in EU human trafficking law and human rights law that are relevant to TIP data collection, which are outlined in Table #3: *Additional European Union legislation relevant to TIP data collection*, below.

Table #3. *Additional European Union legislation relevant to TIP data collection*

European Human Trafficking Law	
CoE (2005) <i>Convention on Action against Trafficking in Human Beings</i> .	The CoE <i>Trafficking Convention</i> sets out a general obligation to “protect the private life and identity of victims” and specifies measures to meet that objective, including setting standards for storage of personal data and ensuring that the media respect the privacy and identity of victims. <sup>137</sup> It sets higher standards for child victims. The CoE <i>Trafficking Convention</i> also states that all personal data regarding trafficked persons is to be in conformity with the <i>Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data</i> (see below), regardless of whether a given state has ratified it. <sup>138</sup>

Court of Human Rights, 4 December 2008, Nos. 30562/04 and 30566/04. FRA (2014) *Handbook on European Data Protection Law*. Vienna, Austria: European Union Agency for Fundamental Rights, pp.145-147.

<sup>135</sup> This Directive repeals the COE Framework Decision 2008/977/JHA, and is broader in scope, also applying to cross-border data and is now recognized as law across the EU along with the GDPR.

<sup>136</sup> See Di Francesco Maesa, C. (2016) ‘Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)’, *Eurojust.it*, May 24.

<sup>137</sup> CoE (2005) *Convention on Action against Trafficking in Human Beings*, ETS No. 197, Article 11. Strasbourg: Council of Europe.

<sup>138</sup> See CoE (2005) *Convention on Action against Trafficking in Human Beings: Explanatory Report*.



EU (2011) <i>Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims</i> (“EU Trafficking Directive”).	Recital 33 of the EU <i>Trafficking Directive</i> explicitly refers to the protection of personal data as recognized by the Charter of Fundamental Rights of the European Union.
<b>European Human Rights Law</b>	
CoE (1950) <i>European Convention on Human Rights</i> .	Article 8 of the <i>European Convention on Human Rights</i> prevents public authorities from interfering with the private life of citizens unless certain conditions have been met: 1. Everyone has the right to respect for his private and family life, his home and his correspondence; 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.
EU (2000) <i>EU Charter of Fundamental Rights</i> .	Under the EU <i>Charter of Fundamental Rights</i> the protection of personal data is considered an autonomous fundamental right, next to the right to privacy. Relevant articles include:  - Article 7: Everyone has the right to respect for his or her private and family life, home and communications. - Article 8: 1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority. - Article 11 of the EU Charter concerns freedom of expression and information, being the ‘freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers’. That right can be limited in exceptional circumstances, including for data protection reasons. <sup>139</sup>



## Africa

Data protection initiatives are uneven across Africa. Some countries have a framework in place; others do not. 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).<sup>140</sup>

Strasbourg: Council of Europe, Article 11:141. St

<sup>139</sup> Also note that Article 16(1) of the *Treaty on the Functioning of the European Union* (TFEU) provides that everyone has the right to protection of personal data concerning him or her. European Union (2012) *Treaty on the Functioning of the European Union*, 2012/C 326/01.

<sup>140</sup> Deloitte (2017) *Privacy is Paramount: Personal Data Protection in Africa*. Johannesburg, South Africa: Deloitte Touche Tohmatsu Limited, p. 7.

While there have been increased efforts in recent years to establish legal frameworks for data protection (with various countries implementing relevant laws), these initiatives do not always have adequate political support or investment of resources for implementation to predict long-term impact.<sup>141</sup> Notwithstanding these limitations, the following initiatives may signify a trend towards further efforts at the regional and sub-regional level, particularly as some countries create data protection authorities, some of which have already joined the *Association Francophone des Autorités de Protection des Données Personnelles* (AFAPDP) that promotes data protection laws and practices in Francophone countries. These laws and regulations have particular relevance and importance in light of recent TIP data collection initiatives being conducted in Africa by governments, international organizations and civil society.

#### Africa Legal Framework

- 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)

#### **African Union Convention on Cyber-security and Personal Data Protection (2014)**

In June 2014, the African Union (AU) adopted its *Convention on Cyber-Security and Personal Data Protection*, which aims to establish regional and legal national legislative frameworks for cyber-security, electronic transactions and personal data protection. While the Convention has been signed by nine of the AU's 55 member states, only one has ratified it.<sup>142</sup> The Convention puts in place a framework for governing data protection, including by requiring states parties to establish a "National Personal Data Protection Authority", an independent administrative authority to oversee that data protection is carried out in accordance with the Convention. A criminalization framework concerning cybercrime and other offences related to information communications technology is also foreseen.

Chapter II of the Convention specifically covers data protection. Article 8 states that each state party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the physical protection of data, and punish any violation of privacy without prejudice to the protection of the free flow of data. In terms of the specific contents of that legislation, the Convention outlines that any data processing mechanism established should respect "the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State and the rights of local communities and the purposes for which the businesses were established."<sup>143</sup> No other guidance is provided on how to reconcile these potentially competing considerations.

Article 10(4) specifies various actions requiring authorization by national authorities, some of which may be relevant to TIP-related data collection, including processing of personal data involving health research, information on offences, convictions or security measures. Further, Article 10(5) states that data relating to prevention, investigation, detection or prosecution of criminal offences or execution of criminal convictions or security measures, that is undertaken on behalf of a government, public institution, local community or private cooperate body operating a public service "shall be in accordance with a legislative or regulatory act enacted after an informed advice of the protection authority". States parties

<sup>141</sup> UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, p. 35.

<sup>142</sup> African Union (2017) *African Union Convention on Cyber Security and Personal Data Protection*. Senegal is the only country to have ratified the Convention to date.

<sup>143</sup> African Union (2017) *African Union Convention on Cyber Security and Personal Data Protection*, Article 8.

are also required to establish a national cyber security policy and strategy (Article 24) and adopt legislation against cybercrime (Article 25).<sup>144</sup>

Article 1 of the Convention defines **personal data** broadly to include “any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.” As with other major instruments on data protection, the Convention outlines basic principles governing the processing of personal data. These include the principle of consent and the legitimacy of personal data processing; lawfulness and fairness; the specific, explicit and legitimate purpose of personal data collection and storage; accuracy; transparency; confidentiality and security (Article 13). The rights of data subjects are set out in Article 16 and include the right to information; the right of access; the right to object; the right of rectification or erasure. Additionally, the Convention sets out specific principles governing processing of **sensitive data**, defined in Article 1 as “all personal data relating to religious, philosophical, political and trade union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions.” Article 14 prohibits the collection of sensitive data,<sup>145</sup> except in a range of situations, some of which may be relevant to TIP-related data. These exceptions include, but are not limited to, instances where a data subject has consented to the collection of sensitive data, when a judicial procedure or criminal investigation has been instituted requiring the collection of sensitive data or when collection of sensitive data is necessary for a task carried out in the public interest.

While the framework provided in the AU Convention goes some way towards protecting data and the rights of data subjects, it will have no practical effect unless it is transposed into the national legislation of states parties.

### ***Supplementary Act A/SA.1/01/10 on Personal Data Protection within Economic Community of West African States (ECOWAS) (2010)***

At the sub-regional level, the Economic Community of West African States (ECOWAS)<sup>146</sup> *Supplementary Act on Personal Data Protection* is a binding regional agreement specifying the required content of data privacy laws. Several member states have enacted legislation to comply with this act. The instrument may be of increasing importance as actors in the ECOWAS region move to improve their data collection and management and as international actors increase data collection (notably on migration related issues) within the ECOWAS region. In recent years in particular, the ECOWAS *Free Movement of Persons’ Protocol* and the ECOWAS *Common Approach on Migration* have triggered increased interest in data on the movement of people and labor markets, particularly from international organizations engaging with stakeholders in the region to increase capacity to collect data on migration management, border management, labor migration and anti-trafficking. In the context of the Free Movement of Persons and Migration in West Africa (FMM West Africa) project (funded by the EU and the ECOWAS Commission and implemented by IOM, ICMPD and ILO), efforts have been made to collect and process standardized migration-related data, including the development of regional guidelines and common operating procedures.<sup>147</sup>

The *Supplementary Act* was strongly influenced by the EU *Data Protection Directive* and replicates many of the principles therein. Article 2 requires member states to “establish a legal framework for protection for privacy of data relating to the collection, processing,

---

<sup>144</sup> AU (2017) *African Union Convention on Cyber Security and Personal Data Protection*, Article 10, 24 and 25.

<sup>145</sup> AU (2017) *African Union Convention on Cyber Security and Personal Data Protection*, Article 1 and 14.

<sup>146</sup> Comprised of Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

<sup>147</sup> FMM West Africa (2017) *Support Free Movement of Persons & Migration in West Africa*.

transmission, storage and use of personal data without prejudice to the general interest of the State.” Articles 14-22 require each member state to establish their own data protection authority and set out the composition, roles and responsibilities of those authorities.<sup>148</sup> As with the AU Convention detailed above, Articles 23-31 of the ECOWAS *Supplementary Act* sets out principles of data protection, including consent and legitimacy; legality and fairness; purpose, relevance and preservation; accuracy; transparency; confidentiality and security and choice of data processor. Articles 38-41 set out the rights of data subjects, including the right to information, the right of access, the right to object and the right to rectification and destruction of data. Finally, Article 32 of the *Supplementary Act* refers specifically to personal data processing carried out for the purpose of journalism, research, artistic or literary expression. Data processing is allowed where it is carried out solely for those purposes and is “in compliance with the ethical rules of these professions”.<sup>149</sup>

### **East African Community (EAC) Framework for Cyber Laws (2009)**

The EAC *Framework for Cyber Laws* recommends that member states develop a regulatory regime for data protection, but does not make specific recommendations.<sup>150</sup> Rather the EAC framework calls for data controllers to comply with “principles of good practice” in processing data, including: accountability, transparency, fair and lawful processing, limitations, data accuracy and data security and to provide copies of personal data to data subjects and allow them to correct inaccurate data.<sup>151</sup> Thus far, there has only been minimal progress in transposing this framework into national legislation, largely owing to the scarcity of resources to invest in the stakeholder consultations needed to enact data protection laws.<sup>152</sup>



### **Asia-Pacific**

In the Asia-Pacific region, there has been a recent surge in data protection frameworks being incorporated into national law, with stronger compliance demanded from governments. Particularly as data technology across the region advances, so too have legislative frameworks evolved to stay abreast of the privacy risks posed, resulting in a range of emerging cyber-security regulatory regimes.<sup>153</sup>

### **Asia-Pacific Legal Framework**

- 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) Privacy Framework (2005)
- Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (2011)

Data privacy regimes have been implemented in all Asia-Pacific Economic Cooperation (APEC) member countries. As

<sup>148</sup> ECOWAS (2010) *Supplementary Act on Personal Data Protection Within ECOWAS*, A/SA.1/01/10. For more on the Supplementary Act, see Ds Isaias Barreto Da Rosa (2016) ‘ECOWAS Supplementary Act A/SA.1/01/10’ in UNCTAD *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, pp. 89-90.

<sup>149</sup> ECOWAS (2010) *Supplementary Act on Personal Data Protection Within ECOWAS*, A/SA.1/01/10.

<sup>150</sup> UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, p. 35.

<sup>151</sup> Makulilo, A.B. (Ed.) (2016) *African Data Privacy Laws*. New York, United States: Springer, p.318.

<sup>152</sup> For more, see Achieng, R. (2016) ‘Data Protection in the East African Community’ in UNCTAD *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, pp.86-88.

<sup>153</sup> Hogan Lovells (2017) *Asia Pacific Data Protection and Cyber Security Guide 2017*. London, United Kingdom: Hogan Lovells.

elsewhere, these are generally underlined by common principles. These frameworks were designed with the interests of cross-border commerce in mind and, as a result, there seems to be lack of clarity and gaps in implementation in the region, particularly in the application of these frameworks to data collection. As in other regions, data protection laws that are in place differ from country to country, some being robust and others less so. Nonetheless, these frameworks and the principles underpinning them offer an important starting point for improved protection of TIP and other data across the Asia-Pacific region.

### **Association of Southeast Asian Nations (ASEAN) Framework on Personal Data Protection (2016)**

In November 2016, at the ASEAN Telecommunications and Information Technology Meeting, the Association of South-East Asian Nations (ASEAN)<sup>154</sup> adopted the *ASEAN Framework on Personal Data Protection*. The framework “serves to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information”. Participants agreed to cooperate, promote and implement in their domestic laws and regulations the Principles of Personal Data Protection, set out in Paragraph 6. As with other instruments, principles address consent, notification and purpose; accuracy; security; accuracy and correction; transfers to other countries; retention and accountability.<sup>155</sup>

To date, the ASEAN Framework is primarily approached through the lens of economic development and cooperation and does not directly address data protection or privacy. However, as stakeholders across the ASEAN region increasingly prioritize data collection in the sphere of trafficking and related fields, the relevance of this framework will need to be fully and explicitly considered. As with other regional mechanisms, the extent to which the ASEAN framework has or will impact TIP data collection activities is dependent on its implementation by member states.

### **Association of Southeast Asian Nations (ASEAN) Convention against Trafficking in Persons (2015)**

The 2015 *ASEAN Convention against Trafficking in Persons, Especially Women and Children* (ACTIP) makes no specific pronouncement on data but does state that its parties shall endeavor to undertake research (Article 11(2)). In line with the United Nations Trafficking in Persons Protocol, the ASEAN Convention also explicitly requires that: “each Party shall protect the privacy and identity of victims of trafficking in persons, including, *inter alia*, by making legal proceedings relating to such trafficking confidential.” However, this privacy is only to be protected “in appropriate case and to the extent possible under its domestic laws” (Article 14(6)). Article 20 of the Convention concerns law enforcement cooperation including through exchange of information. There is no specific data protection provision included, although Article 25 refers to confidentiality of documents, records and information, to be preserved by each party and not “disclosed to or shared with any other Party, State or person except with the prior written consent of the Party which provided such document, record or information.”

The *ASEAN Plan of Action against Trafficking in Persons, Especially Women and Girls* (2015) that complements the Convention, explicitly refers to data collection. Notably, in relation to prevention, the *Plan of Action* refers to collecting suitable data to enable analysis and better understanding of trafficking in persons, and sets out the measure to “Develop national data collection systems in relation to trafficking in persons and methods of exchange of such data between and among ASEAN member states with a view to developing

---

<sup>154</sup> ASEAN is comprised of Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Viet Nam.

<sup>155</sup> ASEAN (2016) *Framework on Personal Data Protection*. Jakarta, Indonesia: Association of South-East Asian Nations.

a regional database for trafficking in persons.” It is otherwise silent on strengthening a data protection framework alongside this endeavor.

### **Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005)**

The Asia-Pacific Economic Cooperation (APEC) region has adopted some key initiatives in data protection, particularly the development of common privacy principles in the *APEC Privacy Framework* in 2005). The *APEC Privacy Framework* has been endorsed by ministers of the region in recognition of the need for effective privacy protections to be developed, without inhibiting economic growth and trade in the APEC region.<sup>156</sup> Published by the APEC Secretariat in 2005, the *APEC Privacy Framework* supports states in setting out clear guidance and direction to businesses on privacy issues and their impact on business, towards developing appropriate privacy protections for personal information and guarding against harmful consequences of its misuse, to harmonize approaches across organizations that collect data in APEC economies and strengthening enforcement of privacy protections.

The *APEC Privacy Framework* is not a legal framework as such. Rather, it considers legislation as one of several options that can be engaged to protect privacy, alongside administrative and self-regulatory options or a combination thereof. Acknowledging of the wide variance across the region, the framework notes:

The Principles have been drafted against a background in which some economies have well-established privacy laws and/or practices while others may be considering the issues. Of those with already settled policies, not all treat personal information in exactly the same way. Some, for example, may draw distinctions between information that is readily searchable and other information. Despite these differences, this Framework has been drafted to promote a consistent approach among the information privacy regimes of APEC economies.<sup>157</sup>

The principles set out in the *APEC Privacy Framework* are consistent with those in the Organization for Economic Cooperation and Development 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.<sup>158</sup> Principles in the *APEC Privacy Framework* include: preventing harm; providing notice to persons about whom information is collected; lawful and fair information collection; accessible information to allow choice; integrity (accurate and up-to-date) personal information; security safeguards (including protection against unauthorized use); access to and correction to information; and accountability (including due diligence in transfer of personal information).<sup>159</sup> Many states have aligned their legislation with the APEC Privacy framework.

### **Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (2011)**

The *APEC Cross-Border Privacy Rules* constitute a self-regulation mechanism that allows data to be transferred between APEC members where a company has voluntarily joined the scheme. To date, only a few countries and businesses have committed to the system. The system provides standard data privacy policies and is meant to facilitate cross-border data transfer and can be referred to in proving compliance with the *APEC Privacy Framework*. Entities can adopt the cross-border privacy principles and then receive accreditation from an approved “Accountability Agent” that recertifies the organization annually. Once an entity is certified as compliant, it is included in a compliance directory. Significant enforcement and compliance challenges of this new mechanism have been noted, raising questions about its long-term potential impact. As of 2016, there were only 13 Accountability Agents, all of

---

<sup>156</sup> APEC (2005) *Privacy Framework*. Asia-Pacific Economic Cooperation Secretariat.

<sup>157</sup> APEC (2005) *Privacy Framework*. Asia-Pacific Economic Cooperation Secretariat, p. 9.

<sup>158</sup> OECD (1980) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, France: Organization for Economic Cooperation and Development.

<sup>159</sup> APEC (2005) *Privacy Framework*. Asia-Pacific Economic Cooperation Secretariat, pp. 11-29.

which were from the United States. Notwithstanding its limitations, its potential to include multi-sector actors is notable.<sup>160</sup>



### Organization of American States

The Organization of American States (OAS) does not yet provide a regional legal framework for data protection. However, in recent years, 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 OAS General Assembly has requested studies to be conducted on issues regarding access to information and data protection issues. The Inter-American Juridical Committee adopted

various resolutions on the issues towards addressing data protection and regional harmonization of OAS member state legislation, including in relation to the private sector.<sup>161</sup>

#### OAS Legal Framework

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

### Organization of American States (OAS) General Assembly Resolutions 2514, 2661 and Principles and Recommendations on Data Protection (2011)

In 2010, the OAS General Assembly requested its General Secretariat to prepare a comparative study of the most prevalent systems for data protection (considering international instruments and national legislations on the topic) for OAS member states to take into account in drafting principles and recommendations.<sup>162</sup>

Via resolution 2661 on “access to personal information and personal data protection,” the General Assembly instructed its Department of International Law<sup>163</sup> to carry out a comparative study of different legal regimes and mechanisms for protecting personal data, with a view to informing the development of a regional framework for OAS states. The study was informed by a questionnaire that OAS member states were requested to complete in relation to their laws, regulations and other relevant mechanisms.

The resulting *Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data)* contain a comparative study of data protection from around the world and offer 15 principles for data protection. The principles include: lawfulness and fairness; purpose of data collection; limitations; transparency; accountability; conditions for processing; disclosures to data processes; international transfers; the right of access; the

<sup>160</sup> UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, pp.34-35.

<sup>161</sup> For more information on the work of the OAS on data protection, see Department of International Law (2017) *OAS: Data Protection*.

<sup>162</sup> OAS (2011) *Draft: Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data)*, Document presented pursuant to General Assembly Resolution AG/RES.2514. “The Inter-American Juridical Committee also adopted several resolutions on this matter, including CJI/RES.9/LV/99, CJI/RES.33 (LIX-O/01), CJI/RES.81 (LXV-O/04) and CJI/RES.130 (LXXI-O/07) to address the regulation of data protection through potential international instruments as well as at the level of the legislation of some OAS member states and of the processing of personal data by the private sector. This work provided valuable input not only to understand the true dimension of this issue in the light of the impact that new technologies have on the expansion of the manipulation and use of the information by individuals, but to help States to take actions regarding law harmonization, improved regional cooperation and finding substantial elements for a future regional instrument on the matter”. See also Department of International Law (2017) *OAS: Data Protection*.

<sup>163</sup> The Department of International Law (DIL) of the Secretariat for Legal Affairs of the OAS promotes the development and codification of international law, both public and private, advises the political bodies of the Organization and serves as Technical Secretariat of the Inter-American Juridical Committee. OAS (2018) ‘Department of International Law’, *Secretariat for Legal Affairs*.

right to correct and delete personal data; the right to object to the processing of personal data; standing to exercise these rights; security measure; duty of confidentiality; and monitoring, compliance and liability.<sup>164</sup>



## 5.4 International law

International law that may apply to TIP data collection ranges from laws specific to human trafficking 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 instruments (as discussed in the previous section) than from international instruments. Nonetheless, 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. The United Nations *Trafficking Protocol* is the first international instrument to provide a definition of trafficking in persons and has 175 states parties (as at December 2019) of whom 158 have criminalized most forms of trafficking in their domestic legislation, in accordance with the Protocol.<sup>165</sup>

Neither UNTOC nor the UN *Trafficking Protocol* (both adopted by the United Nations in 2000) specifically mention data. However, the UNTOC mentions research in the context of cooperation between states parties in planning and implementing research.<sup>166</sup> The *Trafficking Protocol* also mentions research, requiring states parties to “endeavor to undertake measures such as research... to prevent and combat trafficking in persons”. Article 10 states that law enforcement, immigration and other relevant authorities are to cooperate with each other in the exchange of information, in accordance with their domestic law. The *Trafficking Protocol* also require states to “protect the privacy and identity of victims of trafficking in persons” in line with the right to privacy as established in international human rights law.<sup>167</sup>

International human rights law is the body of international law pertaining to state behavior vis-à-vis individuals. The *Universal Declaration of Human Rights* (1948) is generally agreed to be the foundation of international human rights law, with other key international human rights instruments further developing the framework of laws that protect individuals. Among these is the 1966 *International Covenant on Civil and Political Rights* (ICCPR), which states: “No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation”. Also of relevance, is the right to privacy set out in Article 17, stating that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks”.<sup>168</sup>

The Human Rights Committee established by the ICCPR has provided a General Comment

---

<sup>164</sup> OAS (2011) *Draft: Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data)*, Document presented pursuant to General Assembly Resolution AG/RES.2514.

<sup>165</sup> UNODC (2016) *Global Report on Trafficking in Persons*. Vienna, Austria: United Nations Office on Drugs and Crime.

<sup>166</sup> United Nations (2000) *Convention Against Transnational Organized Crime*, A/RES/55/25, Article 29(2).

<sup>167</sup> United Nations (2000) *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*, UN Doc A/45/49, Article 6.

<sup>168</sup> United Nations (1966) *International Covenant on Civil and Political Rights*, A/RES/2200A(XXI), Article 17.



on the right to privacy that clarifies the nature of state obligations with respect to Article 17 and offers significant detail on implementation of the Article. This General Comment states:

The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.<sup>169</sup>

Article 26 of the ICCPR is also of relevance to data protection as it confirms that all persons are equal before the law and entitled to its equal protection. Article 26 prohibits discrimination on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. This provision is increasingly understood to prohibit discrimination, including on the grounds of migration status, meaning, for example, that trafficking victims are entitled to equal protection before the law, including with respect to protection of their data.<sup>170</sup>

The extent to which international human rights law manifests in actual protections of the rights of data subjects ultimately depends on the extent to which these provisions are effectively implemented, both by being incorporated into domestic legislation and through the implementation of that law in practice. Whether this happens varies widely across countries, not only with regard to privacy and data protection, but also more broadly across the gamut of human rights.

---

<sup>169</sup> HRC (1994) *General Comment 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc. ICCPR/C/21/Add. 6, paragraph 10. Geneva, Switzerland: Human Rights Council.

<sup>170</sup> United Nations (1966) *International Covenant on Civil and Political Rights*, A/RES/2200A(XXI), Article 26.



## 5.5 Guidelines, manuals and procedures

How all of these legal frameworks operate in practice (that is, at the institutional or organizational level) varies quite substantially with differences in the practical implementation of these various rules and requirements. Several legal tools exist to support states in the implementation of data protection legislation. For instance, while there is no legally binding regime applicable to the 53 member states of the Commonwealth of Nations (the Commonwealth), it nonetheless has created model laws on privacy and data protection and cybercrime to support harmonization of laws at the domestic level.<sup>171</sup> These instruments, including the *Model Privacy Bill*, *Model Protection of Personal Information Bill*, *Model Freedom of Information Bill* and *Model Law on Computer and Computer Related Crime*, have drawn heavily from OECD Guidelines<sup>172</sup> and replicate principles captured therein.<sup>173</sup>

In addition to overarching laws on data protection and privacy, it is necessary to consider the legislative frameworks for trafficking-related administrative data, including data about victims being assisted either 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). There will be administrative rules, regulations and procedures that operationalize this legislation. These can provide practical guidance on how to adhere to and operationalize the relevant laws and regulations in day-to-day operations. For example, in terms of the collection of administrative data on violence against women, all EU member states have rules regulating administrative data collection and the associated official statistics. These are not usually specified in the legislation but rather captured in national action plans (NAPs) or internal administrative guidelines.

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 in a specific bid to comply with legislation or may exist irrespective of any legislation. Such internal requirements on how such data is collected and managed are not likely to be trafficking-specific but most often will be incorporated into general rules and procedures. For example, at the national level, many state administrative institutions gather TIP-related data, that may accordingly be guided by the administrative guidelines that are specific to their field of work (for example, health, social work or police investigation). Data infrastructures become even more complicated in countries with decentralized governments, where data can be gathered at different levels within the same ministry, but with reporting lines to the regional or provincial government. Depending on the profiles of the professionals who are gathering data, their work may also be influenced by Codes of Conduct that have some impact on data collection.

National statistical offices that regulate the development of general official statistics also have procedures for data collection. In the European Union, these are often mandated by law and the European Statistics *Code of Practice*, which assures the quality of the statistics at the EU standards level and enables comparison.<sup>174</sup> Less guidance exists for civil society

---

<sup>171</sup> The member states of the Commonwealth of Nations span Africa, Asia, the Americas, Europe and the Pacific and are diverse in size and population; 31 member states are classified as “small states” (countries with a population size of 1.5 million people or less). The Commonwealth (2018) ‘Member Countries’, *The Commonwealth*.

<sup>172</sup> OECD (1980) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, France: Organization for Economic Cooperation and Development.

<sup>173</sup> Commonwealth (2016) *Data Protection in the Commonwealth – Key Instruments and Current Practice*. London: Commonwealth Secretariat and UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, p. 36 and pp. 79-82.

<sup>174</sup> EIGE (2016) *Administrative data collection on violence against women: Good practices*. Lithuania: European Institute for Gender Equality.

organizations that also collect administrative data but which may not be bound by the same requirements as state institutions, unless directly funded by the state and contractually/legally bound to follow the same procedures as state agencies.<sup>175</sup> Indeed the guidelines, manuals and procedures that currently exist have been developed to assist NGOs and international organizations in this task but do not provide adequate and universally agreed-upon guidance for those working with TIP-related data, signaling the need for further guidance and tools. Examples of some guidelines, manuals and procedures include, but are not limited to, the materials listed in Table #4, below.

*Table #4. Examples of guidelines, handbooks and manuals on TIP data collection*

<b>Examples of guidelines, handbooks and manuals</b>	
datACT (2015) <i>Data Protection Standards for NGO Service Providers</i> . Germany: KOK and La Strada.	These standards provide guidance to NGO service providers to protect the privacy rights of trafficked persons. They provide basic principles of data collection for NGO service providers from identification through return/social inclusion.
EIGE (2016) <i>Administrative data collection on violence against women: Good practices</i> . Lithuania: European Institute for Gender Equality.	This document addresses gaps and challenges in the collection and analysis of administrative data and provides good practice examples with regard to administrative data collection on violence against women.
ICMPD (2009) <i>Anti-Trafficking Data Collection and Information Management in the European Union – A Handbook: The situation in the Czech Republic, Poland, Portugal and the Slovak Republic</i> . Vienna: International Centre for Migration Policy Development.	This handbook offers guidance to NGOs and governments collecting either victim-centered or criminal justice data and discusses the key legal issues related to data protection including the right to privacy and confidentiality, issues of consent, data storage and maintenance, transmission of sensitive data, information-sharing and exchange, and security in data collection.
ICMPD (2007) <i>Handbook on Anti-Trafficking Data Collection in South-Eastern Europe: Developing Regional Criteria</i> . Vienna: International Centre for Migration Policy Development and NEXUS Institute.	This handbook serves as a practical tool in the implementation of victim-centered and trafficker-centered databases and maps out relevant legal and ethical issues that arise in the collection of TIP data including privacy and confidentiality, consent, security and so on.
IOM (2010) <i>Data Protection Manual</i> . Geneva: International Organization for Migration.	This manual offers practical guidance for protecting personal data in the context of migrant assistance.
IOM (2009) <i>Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators</i> . Vienna: International Organization for Migration and Federal Ministry of the Interior of Austria.	These guidelines provide information pertaining to the protection of personal data, outlining who should have access to the data, the rights of the victims to provide, withdraw or change data and how this data is to be shared and secured.

<sup>175</sup> For example, in the United States, the Violence Against Women Act (VAWA), the Family Violence Prevention and Services Act (FVPSA) and the Victims of Crime Act (VOCA) regulations contain strong confidentiality provisions that limit the sharing of victims' personally identifying information, including entering information into public records and databases. The confidentiality provisions in these regulations apply to all grantees and sub-grantees that are funded by these acts. Most local domestic violence programs in the United States receive VAWA and FVPSA funding through Office on Violence Against Women (OVW) grants and the Department of Health and Human Services (HHS) and therefore must adhere to these regulations. NNEDV (2016) *Confidentiality: VAWA, FVPSA, & VOCA*. United States: NNEDV Safety Net Project and Confidentiality Institute.

<p>KBF &amp; NEXUS (2013) <i>Ethical principles in the re/integration of trafficked persons. Experiences from the Balkans.</i> Washington, D.C.: NEXUS Institute and Brussels: King Baudouin Foundation.</p>	<p>These are ethical principles for the anti-trafficking reintegration field in order to ensure that programs and policies meet the highest human rights standards, offer the highest quality of care and are underpinned by and monitored according to internationally recognized and transparent ethical principles.</p>
<p>KBF &amp; NEXUS (2010) <i>Monitoring anti-trafficking re/integration programmes. A manual.</i> Brussels: KBF &amp; Washington DC: NEXUS.</p>	<p>This manual offers a set of principles to be followed in the collection of administrative data by service providers assisting trafficking victims, along with concrete tools and matrices for monitoring reintegration programs.</p>



## 5.6 Summary

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. Since the 1970s, data protection principles have emerged and been captured in data protection laws and regulations. These are generally conceptualized as privacy law, the broad category of laws that regulate the collection, storage and use of personal information by governments, public organizations or private organizations. While most countries have some privacy laws in place, the extent to which they are comprehensive and effectively implemented varies significantly. Notwithstanding the difference 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. While it is impossible to accurately generalize across national legislation on data protection, key issues in domestic legislation include: scope and applicability, definitions, guiding principles and compliance.

Different regions are at very different stages in the development of legislative and policy infrastructures for data protection. Some regional legislative frameworks are comprehensive. 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, including the recent GDPR. This rigorous framework is manifesting not only in national legislation of EU countries but also in countries elsewhere that are amending their legislation in accordance with the practices and principles that are set out therein. In other regions, legislation is entirely lacking. Moreover, even when regional frameworks do exist, they are not being implemented in practice.

International law that may apply to TIP data collection ranges from laws specific to human trafficking to laws specific to data collection, particularly those protecting the human right to privacy. Notably when it comes to data protection, legislative frameworks at the domestic level more frequently draw from regional instruments than from international instruments. Nonetheless, it is important for data collectors consider the international legal framework for anti-trafficking work and how this 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.

In addition to overarching laws on data protection and privacy, it is necessary to consider the legislative frameworks for trafficking-related administrative data, including data about victims being assisted either 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). There will be administrative rules, regulations, and procedures that operationalize this legislation.

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 the 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. As TIP-related 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-sectoral discussion.

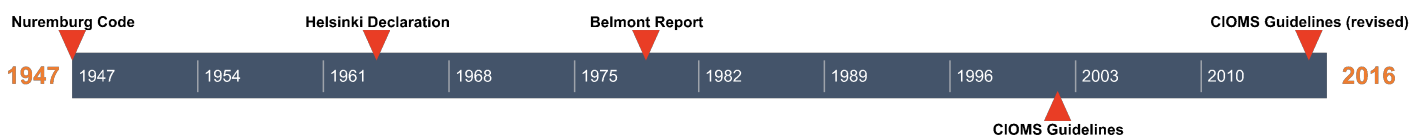


## 6. Ethical Frameworks in TIP Data Collection

Ethical principles should underpin all TIP data collection activities, whether research or administrative data. Each data collection project will need to 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. 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.

There is no universally accepted definition of ethics, but **basic ethical principles** are understood as referring to “those general judgments that serve as a basic justification for the many particularly ethical prescriptions and evaluations of human actions.”<sup>176</sup> 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, which came to the attention of the world during the Nuremberg trials.<sup>177</sup> On the basis of those practices, it was determined that medical research needed to be regulated by ethical principles and standards. The first of those standards to emerge was the Nuremberg Code of 1947 that was drafted during the Nuremberg War Crime Trials as a set of standards for physicians and scientists conducting biomedical experiments.<sup>178</sup> This became the basis for codes that would later emerge to ensure that all research involving human subjects is carried out ethically, key among them being the Helsinki Declaration, Belmont Report and the Council for International Organizations of Medical Sciences (CIOMS) Guidelines as detailed in Table #5, below.

### *Timeline #2. Development of ethical frameworks for data collection*



<sup>176</sup> United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1978) *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Bethesda, United States: National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (“Belmont Report”).

<sup>177</sup> Annas, G.J. and M.A. Grodin (1992) *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation*. Oxford, United Kingdom: Oxford University Press; and Ehrenfreund, N. (2007) ‘How Nuremberg Changed Medical Ethics’ in *The Nuremberg Legacy*. London, United Kingdom: Palgrave, pp.149-152.

<sup>178</sup> Nuremberg Military Tribunals (1949) *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law, No. 10, Volume 2*. Washington, D.C., United States: U.S. Government Printing Office, pp. 181-182.

Table #5. Key ethical standards for research

Standards	Description
World Medical Association Declaration of Helsinki – 1964 (also referred to as the Helsinki Declaration)	A statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data. The Declaration is addressed primarily to physicians, but others involved in medical research involving human subjects are encouraged to adopt the principles. Adopted by the World Medical Association in 1964 and amended several times, most recently in 2013.
Belmont Report – 1979	A summary of research ethics that members of Institutional Review Board (IRB)/ethics review committees are to consider in reviewing research protocols submitted to them. Produced by the United States National Commission for Protection of Human Subjects of Behavioral and Biomedical Research, it sets out three fundamental ethical principles: 1) beneficence, 2) respect for persons, and 3) justice. Much scholarship and subsequent guidance have been dedicated to elaborating the application of these three principles in practice.
International Ethical Guidelines for Biomedical Research involving Human Subjects – 2002 (also referred to as the CIOMS Guidelines)	Guidelines prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO), with commentary on a variety of topics including topics such as ethical review, informed consent, vulnerability of research subjects, equity regarding burdens and benefits etc.). The CIOMS Guidelines give particular attention to applying ethical principles in low and middle-income countries, with different cultures, religions and traditions. Most recently revised in 2016. <sup>179</sup>

The ethical principles laid down in these instruments are of fundamental relevance to data collection, including to the work of researchers who are designing research protocols as well as to Institutional Review Boards (IRBs) and ethics committees responsible for assessing ethical practice. These principles are also relevant to other ethical frameworks, including self-administration of ethics principles and guidelines in data collection and informal peer review mechanisms that may be applied to achieve ethical oversight of data collection activities.

While the origin of research ethics principles is anchored in medical research, it is a continually evolving field with its scope broadening over time. For instance, in 2016, the fourth version of the Council for International Organizations of Medical Sciences (CIOMS) Guidelines included key revisions, one of which was broadening the scope of the initial 2002 guidelines from “biomedical research” to “health-related research”, given that the former was too narrow. Furthermore, what is considered to be “health-related” is also broadening; the Working Group charged with revising the CIOMS guidelines acknowledged that there is no clear distinction between the ethics of social science research, behavioral studies, public health surveillance and the ethics of other research.<sup>180</sup>

Some TIP-related research is being conducted under the umbrella of health research, highlighting the potential applicability of ethics in medical and health-related research to

<sup>179</sup> CIOMS (2016) *International Ethical Guidelines for Health Research involving Humans*. Geneva, Switzerland: Council for International Organizations of Medical Sciences.

<sup>180</sup> CIOMS (2016) *International Ethical Guidelines for Health Research involving Humans*. Geneva, Switzerland: Council for International Organizations of Medical Sciences, p. ix.

other areas of research and data collection, including on TIP. Adaptation of this model to data sciences (including Big Data and Open Data analytics) is less clear as such research is often undertaken by those without experience of applying ethical principles or subjecting their work to ethical review.<sup>181</sup>

Globally there is an increased impetus to strengthen ethical capacity in research and data collection across a range of fields including trafficking in persons. For example, ethics review is increasingly recognized as a safeguard for research subjects. Ethical guidelines and protocols for data collection and the application of human rights standards to data collection activities are increasingly common for research as well as administrative data collection.<sup>182</sup> In the meantime, while lacuna still remain in ethical oversight of TIP research and data collection, practitioners have applied other informal channels and *ad hoc* approaches to ensure that their data collection activities comply with ethical principles and standards.

Ethics and ethical issues that may arise for all of the variations of TIP data collection must be carefully thought through and applied in different ways. While many issues are common across a range of data collection activities and the ethical guidance is generally adaptable and transferable to how TIP data collection may be done, ethical frameworks are not black and white. The evolving and divergent nature of what constitutes TIP data collection adds another layer of complexity to be explored and addressed. There is an emerging body of literature that explores the complex ethical issues that arise in TIP research and data collection.<sup>183</sup>

---

<sup>181</sup> Leetaru, K. (2017) 'Is it too late for Big Data Ethics?', *Forbes*, October 16.

<sup>182</sup> See Table #6, *Guidelines on the ethical collection of TIP data*.

<sup>183</sup> This includes, but is not limited to: Bilger, V. and I. van Liempt (2009) 'Introduction' and 'Methodological and ethical dilemmas in research among smuggled migrants' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press; Boyd, Z. and K. Bales (2016) 'Getting What We Want: Experience and Impact in Research with Survivors of Slavery' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 173-190; Brunovskis, A. (2012) 'A penny for your thoughts – paying participants in research' ['å betale deltakere i forskning'] in Fossheim, H. and H. Ingierd (Eds.) *Research and Money [Forskning og penger]*. Norway: Forskningsetiske komiteer; Brunovskis, A. (2010) 'Irregular Migration Research in Norway: Reflections on Research Ethics and Methodological Challenges Based on a Methods Development Project in Norway' in Thomsen, T. et al. (Eds.) *Irregular Migration in a Scandinavian Perspective*. Maastricht, Netherlands: Shaker Publishing; Brunovskis, A. and R. Surtees (2010) 'Untold Stories: Biases and Selection Effects in Research with Victims of Trafficking for Sexual Exploitation', *International Migration*, 48(4), pp. 1-37; Coy, M. (2006) 'This morning I'm a researcher, this afternoon I'm an outreach worker: Ethical dilemmas in practitioner research international journal of social research methodology', *Theory and Practice*, 9(5), pp. 419–432; Cwikel, J. and E. Hoban (2005) 'Contentious issues in research on trafficked women working in the sex industry: Study design, ethics and methodology', *The Journal of Sex Research*, 42(4), pp. 306–316; Dahinden, J. and D. Efiionayi-Mader (2009) 'Challenges and strategies in empirical fieldwork with asylum seekers and migrant sex workers' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press; De Wildt, R. (2016) 'Ethnographic Research on the Sex Industry: The Ambivalence of Ethical Guidelines' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 51-70; Duong, K.A. (2015) 'Doing Human Trafficking Research: Reflections on Ethical Challenges', *Journal of Research in Gender Studies*, 5(2), pp. 171-190; Easton, H. and R. Matthews (2016) 'Getting the Balance Right: The Ethics of Researching Women Trafficked for Commercial Sexual Exploitation' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 11-32; English, A. (2017) 'Mandatory Reporting of Human Trafficking: Potential Benefits and Risks of Harm', *AMA Journal of Ethics*, 19(1); GAATW (2015) *Briefing Paper: Seeking Feedback from Trafficked Persons on Assistance Services: Principles and Ethics*. Bangkok, Thailand: Global Alliance Against Traffic in Women; Guillemin, M. and L. Gillam (2004) 'Ethics, reflexivity and "ethically important moments"', *Research in Qualitative Inquiry*, 10(2), pp. 261–280; Horning, A. and A. Paladino (2016) 'Walking the Tightrope: Ethical Dilemmas of Doing Fieldwork with Youth in US Sex Markets' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 205-226; Hynes, P. (2017) 'Trust and mistrust in the lives of forcibly displaced women and children', *Families, Relationships and Societies*, 6(2); Kelly, L. and M. Coy (2016) 'Ethics as Process, Ethics in Practice: Researching the Sex Industry and Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 33-50; Kerrand, P.L. and R. Dash (2017) 'Ethical Considerations in Mandatory Disclosure of Data Acquired While



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. On this point, the OHCHR's *Recommended Principles and Guidelines on Human Rights and Human Trafficking* underscore the importance of ethical collection of data, emphasizing that anti-trafficking strategies must be based on accurate and current information, experience and analysis. The OHCHR Guidelines call for states and, where appropriate, intergovernmental and non-governmental organizations to consider:

...undertaking, supporting and bringing together research into trafficking. Such research should be firmly grounded in ethical principles, including an understanding of the need not to re-traumatize trafficked persons. Research methodologies and interpretative techniques should be of the highest quality.<sup>184</sup>

---

Caring for Human Trafficking Survivors', *AMA Journal of Ethics*, 19(1); Lewis, H. (2016) 'Negotiating Anonymity, Informed Consent and 'Illegality': Researching Forced Labour Experiences Among Refugees and Asylum Seekers in the UK' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 99-116; Marcus, A. and R. Curtis (2016) 'No Love for Children: Reciprocity, Science, and Engagement in the Study of Child Sex Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 191-204; Markova, E. (2009) 'The "insider" position: ethical dilemmas and methodological concerns in researching undocumented migrants with the same ethnic background' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press; McAdam, M., R. Surtees and L.S. Johnson (2019) *Legal and Ethical Issues in Data Collection on Trafficking in Persons*. Washington, D.C.: NEXUS Institute; Melrose, M. (2002) 'Labour pains: Some considerations on the difficulties of researching juvenile prostitution', *International Journal of Social Research Methodology*, 4(4), pp. 333-351; Moniruzzaman, M. (2016) 'At the Organ Bazaar of Bangladesh: In Search of Kidney Sellers' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 227-248; Rothman, E.F. et al. (2018) 'Ethical and Practical Considerations for Collecting Research-Related Data from Commercially Exploited Children', *Behavioral Medicine*, 44(3), pp. 250-258; Scheper Hughes, N. (2016) 'On Adopting Heretical Methods: From Barefoot to Militant to Detective Anthropology' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 249-272; Scott, S. and A. Geddes (2016) 'Ethics, Methods and Moving Standards in Research on Migrant Workers and Forced Labour' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 117-136; Siegel, D. (2016) 'Ethnicity, Crime and Sex Work: A Triple Taboo' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 71-84; Siegel, D. and R. de Wildt (2016) 'Introduction: The Variety of Ethical Dilemmas' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 1-7; Staring, R. (2009) 'Different methods to research irregular migration' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press; Surtees, R. (2014) 'Another side of the story: challenges in research with unidentified and unassisted trafficking victims' in Yea, S. (Ed.) (2017) *Human Trafficking in Asia: Forcing Issues*. New York: Routledge; Surtees, R. and A. Brunovskis (2016) 'Doing No Harm - Ethical Challenges in Research with Trafficked Persons' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 137-154; Surtees, R. and S. Craggs (2010) *Beneath the surface. Methodological issues in research and data collection with assisted trafficking victims*. Geneva, Switzerland: International Organization for Migration and Washington, D.C.: NEXUS Institute; Tyldum, G. (2012) 'Ethics or access? Balancing informed consent against the application of institutional, economic or emotional pressures in recruiting respondents for research', *International Journal of Social Research Methodology*, 15(3); Warden, T. (2013) 'Feet of clay: confronting emotional challenges in ethnographic experience', *Journal of Organizational Ethnography*, 2(2), pp. 150-172; Yea, S. (2016) 'Trust, Rapport, and Ethics in Human Trafficking Research: Reflections on Research with Male Laborers from South Asian in Singapore' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 155-172; Zhang, S.X. (2016) 'The Ethical Minefield in Human Trafficking Research - Real and Imagined' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 85-98; and Zimmerman, C. and C. Watts (2004) 'Risks and responsibilities: guidelines for interviewing trafficked women', *Lancet*, 363(9408).

<sup>184</sup> OHCHR (2002) *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, UN Doc E/2002/68/Add.1[4], Guideline 3.

The following sections describe different approaches to ensure ethical data collection on trafficking in persons, including: ethics review; research and data collection partnerships; self-administered ethical standards and guidelines; peer review procedures; and informal third-party engagement in protection. In some cases, a combination of more than one approach may be utilized in undertaking a data collection initiative.

#### Different approaches to ensure ethical data collection on TIP

- Ethics review
- Research and data collection partnerships
- Self-administered ethical standards and guidelines
- Peer review procedures
- Informal third-party engagement in protection



### 6.1 Ethics review

Ethics review is the review and approval (or rejection) of research proposals and oversight of research activities. Most commonly this is through Institutional Review Boards (IRBs),<sup>185</sup> generally established at universities to review research conducted by that institution. Some IRBs have been established to provide ethical oversight to the research and data collection work in international or multi-country contexts. While not yet the case in the field of TIP, this offers one possible way forward as attention to ethics and the demand for ethics review gain traction in the anti-trafficking field (for research as well as other types of TIP data collection). There are also private, independent IRBs that are not affiliated with any particular institution but that provide ethics review services, although none specialized in the field of human trafficking.

Different IRBs are governed by different procedures in how they carry out review. Many institutions refer to the *Belmont Report* as their statement of principles or to the *Helsinki Declaration* or CIOMS as their statement of assurance, while others may formulate their own statement of principles and be guided by them in their work.<sup>186</sup> IRB membership is generally governed by a set of standards establishing the number and composition of its members, which may include a representative of the community relevant to the study (for example, former trafficking victims or anti-trafficking professionals). Alternatively, IRBs may have a mechanism for consulting with subject experts on a case-by-case basis. One

<sup>185</sup> Also sometimes called independent ethics committees (IECs), ethical review boards (ERBs) or research ethics boards (REBs).

<sup>186</sup> IRBs should have written procedures in place and clear standards that can be referred to in ensuring that members apply national, regional and international standards, guidelines and laws in a consistent, transparent and coherent way. WHO (2011) *Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants*. Geneva, Switzerland: World Health Organization, p. 10, Standard 6 and pp.30-36. In the United States Federal system, research involving human subjects that a U.S. Federal government department conducts, supports or otherwise regulates is governed by the “Common Rule” (Code of Federal Regulations Title 45 Part 46 – Protection of Human Subjects). The Common Rule sets out criteria for establishing IRBs as well as rules on specific considerations in ethical research, including as informed consent processes, weighing of risks and benefits and recruitment of human subjects. Government of the United States (2017) ‘Federal Policy for the Protection of Human Subjects’, *Federal Register 87(12)*, pp. 7149-7274. Washington, D.C.: U.S. Government. The Common Rule requires that in order to assure compliance, an IRB adheres to a statement of principles that may include a statement of ethical principles. Government of the United States (2009) *Code of Federal Regulations*, Title 45, Part 46, Section 46.103(b)(1). Washington, D.C., United States: U.S. Government. Changes to the Common Rule were published on 19 January 2017. Those changes include additional requirements for consent forms, use of a single IRB for multi-institutional research studies, and, in the case of studies on stored identifiable data, the option of relying on broad consent obtained for future research as an alternative to seeking IRB approval to waive consent requirements. New exemption categories are also established based on the level of risk posed to participants, to reduce unnecessary regulatory burdens on IRBs.

researcher working with vulnerable populations described one such variation that may be useful for some TIP research projects:

Our IRB has allowed in certain instances for community consultation boards to be developed. They want to make sure they're independent, they're not just a rubber stamp, but that provides for an effective process of documenting local IRB oversight, but giving some flexibility in different contexts to say here's a marginalized population that for whom a local IRB really doesn't exist or would not be representative... [my university] would be the IRB of record, but [we would also develop] a local community IRB formed by [community members] who would say: "I know that experience, I have lived in that context and I understand those dynamics" and can assist in either saying "stop this interview or stop this research, it's too risky" or how to protect those populations. We want to give agency to those entities that are in a best position to protect the human subjects and not just either rubber stamp it or arbitrarily because of our own vested interest say "no".

While common for universities, IRBs are not generally available for research and data collection being conducted by NGOs, international organizations or the United Nations. Most organizations do not have access to a process of ethics review when not affiliated or partnering with an academic institution. As one researcher noted:

...many nonprofit [organizations] they just don't have access to IRBs, because they're not academically affiliated or they're not a scientific research organization.

There may also be a system of rules and procedures for ethics review in the country where research takes place. National ethics review bodies may be able to provide more tailored reviews than international IRBs can, due to their local expertise and familiarity with contextual considerations and risks. However, relatively few countries around the world enforce IRB-level ethics review over non-medical research.<sup>187</sup> One NGO researcher described difficulty in accessing ethics review bodies and procedures when conducting TIP research in different countries:

A lot of the places where we work don't have [the ethics review] institution or, if they do, they are not functional... we actually tried to go through this process in [one country] and all of the places where we could find some sort of ethical review. They asked why were we submitting to them because they do more research on health... This is something that we're struggling through.

Another NGO researcher described the arduous experience of ethics review, as the only available ethics review process in the country where research was conducted was the health research review board, which had no knowledge or experience of TIP research:

...the only way that we could go through ethics review [was to] go through the Ministry of Health here, which is the only government ministry that has an ethics review board... [It didn't really] fit very well into the Ministry of Health because of the focus of the research [on human trafficking].

To benefit TIP research, any ethics review body should have knowledge of TIP and the specific ethical issues that arise in TIP research to be able to determine what are or are not appropriate ethical procedures, particularly when conducting research with human subjects. Questions have been raised as to the extent to which existing ethics review bodies have the

---

<sup>187</sup> As the National Science Foundation (NSF) in the United States notes, "many foreign countries IRBs [sic] deal only with biomedical research and will refuse to extend their purview to cover social and behavioral science. In other foreign situations there will be no analogue to an IRB and the concept may be irrelevant". Leetaru, K. (2016) 'Are Research Ethics Obsolete in the Era of Big Data?', *Forbes*, June 17.

experience and understanding of the specificities of trafficking research to be able to provide constructive or useful reviews.<sup>188</sup> As such, ethics approval may not always guarantee that research is ethical. One TIP researcher argues as follows:

...the development of IRBs, which have metastasized across the entire academic world, have now assumed all authority in adjudicating and imposing ethical conduct of all research endeavors involving human subjects...It is not that the idea of enforcing a code of ethical conduct in a research community is a bad one. It is the process by which people with little research experience or inadequate understanding of the subject matter convene to determine what are or are not ethical field procedures.<sup>189</sup>

Ethics review bodies in more politically constrained countries may place restrictions on conducting research which they deem “political” or “sensitive”, rejecting it not on the basis of ethics but on other disingenuous grounds. This is worth attention given that TIP as a field is susceptible to ideological orientations and a range of political sensitivities.

Ethics review processes do not always align with the reality of how TIP research is conducted, including when data collection has short timelines and limited funds and is frequently at the behest of donors and contracting organizations. Time and funding are often not allocated to proceed with ethics review. As one researcher noted:

Most of the studies that are done... don't get some kind of external ethical approval. [...] And I know often, again with contracted research there is a time pressure. You have to produce this report [quickly].

Ethics procedures may also not readily fit with data that is collected with and through organizations engaged in operational anti-trafficking work. While some of this data is then used for research, it is not only a research endeavor and it is unclear how ethics review may be undertaken in this context.

TIP research implies different levels of ethical risks, which may require different levels and types of ethics review and ethics procedures. This aligns with observations of one research body which noted the following:

...[IRBs] has been long critiqued for being ill-suited for models of inquiry that follow non-biomedical procedures for interacting with people...Many regulatory bodies across the world have dealt with these issues by creating different levels of ethics board review based on the idea that some research might be exempt from review or require only limited review.<sup>190</sup>

---

<sup>188</sup> Marcus, A. and R. Curtis (2016) ‘No Love for Children: Reciprocity, Science, and Engagement in the Study of Child Sex Trafficking’ in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. New York, United States: Springer, pp. 197-198; and Zhang, S.X. (2016) ‘The Ethical Minefield in Human Trafficking Research - Real and Imagined’ in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. New York, United States: Springer, p.92.

<sup>189</sup> Zhang, S.X. (2016) ‘The Ethical Minefield in Human Trafficking Research - Real and Imagined’ in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. New York, United States: Springer, p.92.

<sup>190</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, pp. 6-8.

In lieu of an ethics review body, some international NGOs in the health field have established their own ethics review mechanisms. This is an expensive, time-consuming and complex avenue to pursue and, as such, may only be an option in the case of large and well-funded organizations. Given the very recent nature of this approach even within well-established professional fields and among large and well-funded organizations, it is perhaps not surprising that this practice has not yet emerged in the TIP field. However, as this constitutes an opportunity for good practice in the future, lessons can be drawn from the health field.<sup>192</sup>

**Box #7. Example of an internal ethics review process**

Plan International’s Research Policy and Code of Conduct is an internal ethics review process. Research involving human subjects must receive ethics approval. Where external ethics approval cannot be obtained, ethics approval from the Research and Knowledge Management Team and Plan International Headquarters must be obtained. Approval is given in writing and reasons are provided if approval is declined.<sup>191</sup>

Another approach is for organizations to establish a formal process of internal ethics review, as illustrated in Box #7. An internal ethics review process provides an organization with a system of checks and balances that they may not have access to through the more traditional, academically oriented review procedures. This approach has been endorsed by the Australian Council for International Development, which has stated in its principles and guidelines that:

Research is often considered of “negligible risk” where any foreseeable risk is no more than inconvenience and “low risk” where the only foreseeable risk is discomfort. In these cases, a reduced or internal assessment of ethical issues may be considered rather than a formal ethical review and approval. Such cases might apply to evaluation or research processes that address non-sensitive issues or topics, do not involve vulnerable groups and use minimal participant time. Further, such an internal assessment might be considered for well-established evaluation methods and where the aim or purpose of the research is to improve the implementation of an established intervention or program (quality assurance).<sup>193</sup>

In sum, various types of formal ethics review bodies and models may be leveraged in conducting TIP research. There is no one-size fits all approach.

In the context of emerging forms of TIP data collection (as discussed in Section 7), ethics review does not always keep pace with new technologies. Even within universities, some types of 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. One technology expert observed the following:

...at the majority of universities I’ve spoken with over the past year, computer science research is rarely subjected to ethical review, meaning that the majority of the daily

<sup>191</sup> Plan International (2013) *Research Policy and Code of Conduct*. United Kingdom: Plan International, p.9.

<sup>192</sup> In the field of health services and humanitarian service delivery some (generally large and well-funded) organizations have established ethics review mechanisms to oversee the research and data collection components of their work. Examples in the field of health services include Family Health International, Population Council, Population Services International and Marie Stopes International (MSI). In the field of humanitarian service delivery, much can be learnt from the pioneering work of Medicines Sans Frontiers (MSF) in establishing an ethics review board and adapting its procedures to the nature of its work, which is often conducted in emergency contexts. See Schopper, D. et al. (2009) ‘Research ethics review in humanitarian contexts: The experience of the independent ethics review board of Medecins Sans Frontieres’ *PLOS Medicine*, 6, and Sheather J. et al. (2016) ‘A Médecins Sans Frontières Ethics Framework for Humanitarian Innovation’ *PLOS Medicine* 13(9). See also Testa, A.C. et al. (2011) *A Matter of Principle: A Family Planning NGO Experience Setting up an Independent Ethics Review Committee (Poster)*. United States: Advancing Ethical Research Conference.

<sup>193</sup> ACFID (2016) *Principles and Guidelines for ethical research and evaluation in development*. Australia: Australia Council for International Development, p.18.

advances in artificial intelligence [AI] have likely never been subjected to ethical review of any kind. At the same time, the AI research which does find itself forwarded to an IRB is typically exempted from actual review by virtue of involving publicly accessible data, meaning that precious few of the actual questions being explored in AI research today have ever actually undergone even the most cursory of ethical review.<sup>194</sup>

The same technology expert noted that some funders attempt to exempt an ever-widening category of research from ethics review and some prominent journals do not require ethical review on the basis of the international scope of their authorship.<sup>195</sup> Questions arise as to the point at which human subjects data is sufficiently transformed to no longer be subject to IRB or ethics approval.<sup>196</sup>



## 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. For example, when an organization partners with or engages an independent university or research institute to carry out research, ethics approval may be sought from that institution. As one staff of a UN agency noted:

We've adopted [ethical protocols] when we've had research partners. We did a piece of research with [a university], we adopted their ethical guidance. We're trying to draw and benefit from what already is out there.

In other 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. One UN project focused on anti-trafficking in Asia developed ethical guidance<sup>197</sup> to be used in research and data collection done by NGOs which they fund and work with, as one staff explained:

...it's a relatively straightforward tool, seven standards or guidelines and so you can apply that to various different audiences...the [guide] comes with an ethics review process that is encouraged to be implemented whenever there's nothing else in place... So, what we do in house, all research that we conduct goes through that. [...] We go through all of those different points explained in the [guide]... And then we have a process whereby we go back and forth to discuss some of those approaches that are laid out in the review form for that particular type of research and clarify a couple of points where there may be a need to do so.

---

<sup>194</sup> Leetaru, K. (2017) 'AI "Gaydar" and How the Future of AI will be Exempt from Ethical Review', *Forbes*, September 16. The use of Big Data in TIP data collection is gaining ground and the specific ethical and legal issues at play are discussed in more detail below (see Section 7.2 *Using Big Data in anti-trafficking work*).

<sup>195</sup> Leetaru, K. (2017) 'Is it too late for Big Data Ethics?', *Forbes*, October 16.

<sup>196</sup> Leetaru, K. (2016) 'Are Research Ethics Obsolete in the Era of Big Data?', *Forbes*, June 17.

<sup>197</sup> UNIAP (2008) *Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming*. Bangkok, Thailand: United Nations Inter-Agency Project on Human Trafficking. The UNIAP Guide is also available in Burmese, Chinese, Vietnamese, Cambodian and Thai.

Engaging researchers with experience in ethical principles and approaches to TIP data collection can also introduce ethical oversight for 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 it may otherwise be lacking. One researcher highlighted the value of these partnerships toward more ethical TIP data collection:

...we see in this area a lot of the work, particularly on the protection side and assisting survivors, being done by NGOs. And many of them are sitting on a lot of data. What that data looks like, I can't speak to, but I think there's value in partnering with academic researchers who can understand, who can help with this evaluation of data. ...even if they're working privately and so are not implicated by the ethics regulations, they ought to be going through that process or a parallel process to ensure that they're able to confidently say that their research was done ethically.

Some organizations conduct research and data collection in partnership with government ministries involved in the anti-trafficking response in the country. Depending on the topic of data collection, this might include ministries of social affairs, labor, health, education, gender/women's affairs, child protection/affairs, interior, justice and so on. These government agencies may offer some form of ethical oversight, both as a result of administrative rules as well as given the particular expertise on TIP and familiarly with the local context and ethical risks and other considerations that may arise.

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. One researcher described the value in partnerships between service providers and researchers not only in the initial ethical framing of the project but also in ensuring that data and research are used to positive effect:

I like the idea of the organizations that are providing those services, whether they be governmental, non-governmental, partnering with researchers to decide together what the agencies need to know in order to provide those services more effectively. And then partnering with people who have the research skills to help them be able to actualize that. And then making sure that that research that is conducted is actually used. And so, from my perspective as an academic, it's actually very, very hard to do this well because within academia the incentive structure is set up such that you need to crank out your publications and move on. And ethically that's not okay with me. I think it's really important that we focus on research uptake, that we're taking these studies that we've worked on collaboratively with agencies actually providing those protection services and then we disseminate it in an efficient manner and then use it to inform [policies] better or differently in the future.

Another possible partnership model involves working with vulnerable persons or communities to determine how data is collected. As noted in a guidance note on data collection:

Decisions concerning data collection on particularly vulnerable or marginalized groups, including, 'legally' invisible groups for instance, should be made in close partnership or consultation with the group concerned to mitigate associated risks".<sup>198</sup>

That being said, partnerships (in the various forms discussed above) may serve to facilitate research or data collection, but not necessarily or automatically strengthen its ethics. It is the

---

<sup>198</sup> OHCHR (2016) *A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance Note to Data Collection and Disaggregation*. Geneva, Switzerland: Office of the United Nations High Commissioner for Human Rights, p. 7.

specific nature of the partnership and the mechanisms and tools used that will serve to rise to the level of 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 may risk diluting ethical standards when responsibilities are allocated to the partner that has least capacity to fulfill them. For instance, a government department, academic or other research entity may allocate informed consent responsibilities to a partnering NGO that has direct contact with research subjects, but little expertise to do so. In such situations, questions that should be asked include: what responsibilities do both parties have? Does the more capable partner or the funding partner retain accountability for what its implementing partner does with data and how it is collected? What ethical and legal obligations arise when one party to the arrangement knows that the NGO may not obtain adequate informed consent? 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 to ensure informed consent).



### 6.3 Self-administered ethical standards and guidelines

Another approach is the adaptation and application of ethical principles to the design and conduct of TIP data collection activities. This is largely self-administered and may be *ad hoc* in nature. It may involve individuals engaged in a given activity who look 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, when internal policy guidelines specify which external ethics guidelines are to be complied with in the context of the research or data collection initiative).

Ethical standards and guidelines 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 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).

The above issues notwithstanding, there are some self-administered tools and guidance that are currently used by frontline data collectors and researchers in the TIP data collection field, as outlined in Table #6: *Guidelines for the ethical collection of TIP data* below. For instance, the *UNIAP Guide to Ethics and Human Rights in Counter Trafficking* is self-administered ethical guidance for data collectors engaged in counter trafficking research and programming.<sup>199</sup> The *WHO Ethical and Safety Recommendations for Interviewing*

---

<sup>199</sup> UNIAP (2008) *Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming. Ethical Standards for Counter-Trafficking Research and Programming*. Bangkok, Thailand: United Nations Inter-Agency Project on Human Trafficking. See also Rende-Taylor, L. and M. Sullivan (2012) 'Raising the Standard of Ethics and Human Rights Among Anti-human Trafficking Responders in the Mekong Region', *Human Rights Education in Asia-Pacific*, 3, pp. 55-69.



*Trafficked Women* offer guidance on how to interview trafficked women and cover core ethical issues such as “do no harm”, assessing risk, informed consent, data protection and using information in an ethical way.<sup>200</sup> Similarly, UNICEF’s *Guidelines on the Protection of Child Victims of Trafficking* include a list of questions and ethical considerations when conducting research on child trafficking, with issues related to whether it is suitable to engage children in the research and, if so, how this can be done to avoid harm to the child.<sup>201</sup> And the Global Alliance Against Traffic in Women (GAATW) drafted a paper outlining the ethical challenges that researchers/service providers identified through a participatory research project by member organizations, interviewing 121 trafficking victims, around the world.<sup>202</sup>

Table #6. Guidelines on the ethical collection of TIP data

<b>Guidelines relevant to ethical collection of data specific to human trafficking</b>	
datACT (2015) <i>Data Protection Standards for NGO Service Providers</i> . Germany: KOK and La Strada.	Guidelines for NGOs specifically on data collection principles in initial identification; during counseling; on providing information on data protection to trafficked persons; in return and social inclusion and in national reporting mechanisms.
ECPAT International (2019) <i>Ethical considerations in research on sexual exploitation involving children</i> . Bangkok, Thailand: ECPAT International.	Critical ethical considerations for research on sexual exploitation that involves children.
GAATW (2015) <i>Briefing Paper: Seeking Feedback from Trafficked Persons on Assistance Services: Principles and Ethics</i> . Bangkok: Global Alliance Against Traffic in Women.	Principles and ethical guidance based on 121 interviews conducted by GAATW in 2013 of trafficked women, men and girls in Latin America, Europe and Asia to learn their experiences of assistance interventions.
ILO (2012) ‘Ethical rules for conducting a survey on forced labour’, <i>Harder to see, harder to count: survey guidelines to estimate forced labour of adults and children</i> . Geneva: International Labour Organization, pp. 89-92.	Rules on the special case of surveys of forced labor of children that were initially designed by ILO for surveying the worst forms of child labor in Nepal. These ethical rules are primarily relevant to interviews with victims and perpetrators.
IOM (2009) <i>Caring for Trafficked Persons: Guidance for Health Providers</i> . Geneva: International Organization for Migration.	Guidelines on safety, referral, confidentiality and privacy; providing information to trafficked persons; informed consent; appropriate interview practices.
IOM (2009) <i>Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators</i> . Vienna: International Organization for Migration and Federal Ministry of the Interior of Austria.	The Guidelines seek to enhance the capacity of national authorities to collect and share data as well as to contribute to EU-wide efforts to enhance data collection, protection and to foster cooperation.
Issara Institute (2018) <i>Updated Guide to Ethics &amp; Human Rights in Anti-Trafficking</i> . Thailand: Issara Institute.	This guide builds on UNIAP’s <i>Guide to Ethics and Human Rights in Counter-Trafficking</i> and includes new sections and case studies on corporate responsible sourcing and data ethics.

<sup>200</sup> WHO (2003) *Ethical and Safety Recommendations for Interviewing Trafficked Women*. Geneva, Switzerland: World Health Organization.

<sup>201</sup> UNICEF (2006) *Guidelines on the Protection of Child Victims of Trafficking*. New York, United States: United Nations Children’s Fund.

<sup>202</sup> GAATW (2015) *Briefing Paper: Seeking Feedback from Trafficked Persons on Assistance Services: Principles and Ethics*. Bangkok, Thailand: Global Alliance Against Traffic in Women.

KBF & NEXUS (2010) <i>Monitoring anti-trafficking re/integration programmes. A manual</i> . Brussels: King Baudouin Foundation and Washington, D.C.: NEXUS Institute.	This manual includes a chapter on ethical principles in the collection of administrative data about trafficking victims, collected in the context of assistance and reintegration programs.
Liberty Asia (2015) <i>Data Protection Guidelines</i> . Hong Kong: Liberty Asia.	These Guidelines aim to clarify the protections available in Hong Kong's data protection law and to assist NGOs with protecting sensitive data.
OHCHR (2002) <i>Recommended Principles and Guidelines on Human Rights and Human Trafficking</i> , UN Doc E/2002/68/Add.1[4].	Guideline 3 concerns research, analysis, evaluation and dissemination.
UNIAP (2008) <i>Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming</i> . Bangkok: United Nations Inter-Agency Project on Human Trafficking.	Seven principles on ethics and human rights in anti-trafficking including a self-administered ethics review form template for researchers to voluntarily complete.
UNICEF (2006) <i>Guidelines on the Protection of Child Victims of Trafficking</i> . New York: United Nations Children's Fund.	Section 12 concerns ethics in research and data collection, including principles such as "doing no harm", informed consent, providing information and avoiding raising unrealistic expectations of subjects.
WHO (2003) <i>Ethical and Safety Recommendations for Interviewing Trafficked Women</i> . Geneva: World Health Organization.	These recommendations provide ten basic standards for interviewing trafficked women.

There are also some self-administered guidelines that can be utilized when collecting data for monitoring and evaluation. For instance, as part of its regional program on the reintegration of trafficking victims, the King Baudouin Foundation funded the development of a monitoring manual for implementing partners, which includes ethical principles in the collection of administrative data about trafficking victims, collected in the context of reintegration programs.<sup>203</sup> Some individual organizations (for example, Plan International) have also developed materials for how to address ethics within the framework of monitoring their programs.<sup>204</sup> And while not specific to TIP, several associations of evaluators have developed ethical guidance in conducting evaluations.<sup>205</sup> 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. As one team of researchers explained of their experience:

... as a first step in developing our research with victims of trafficking, we reviewed both the British Society of Criminology's *Code of Ethics for Researchers in the Field*

<sup>203</sup> KBF & NEXUS (2010) *Monitoring anti-trafficking re/integration programmes. A manual*. Brussels, Belgium: King Baudouin Foundation and Washington, D.C., United States: NEXUS Institute.

<sup>204</sup> Plan (2009) *How to: Include Child Protection in All Monitoring, Evaluation and Research Initiatives*. Woking, United Kingdom: Plan Ltd. Unpublished document; and Plan (2009) *How to: Include Ethical Standards in all Monitoring, Evaluation and Research Initiatives*. Woking, United Kingdom: Plan Ltd. Unpublished document.

<sup>205</sup> AfreA (2002) *The African Evaluation Guidelines*. Accra, Ghana: African Evaluation Association; AEA (2004) *American Evaluation Association Guiding Principles for Evaluators*. United States: American Evaluation Association; and AES (2010) *Guidelines for the Ethical Conduct of Evaluations*. Lyneham, United Kingdom: Australasian Evaluation Society, Inc.

of *Criminology* (2006) and the available research methods literature about conducting sensitive research with vulnerable populations.<sup>206</sup>

Guidelines for ethical data collection that are not specific to human trafficking are included in Table #7 below. This is a non-exhaustive list intended as a resource on guidelines for ethical data collection.

Table #7. Guidelines for ethical data collection, not specific to human trafficking

<b>Guidelines relevant to ethical collection of data (not specific to human trafficking)</b>	
Accenture (2016) <i>Universal principles of data ethics: 12 guidelines for developing ethics codes</i> . Beaverton: Accenture.	This report discusses the dynamics involved in generating a code of ethics that could guide the profession of data science as it grows and evolves and immediately help organizations shape their own internal guidelines related to data. A broad set of principles is proposed.
ACFID (2016) <i>Principles and Guidelines for ethical research and evaluation in development</i> . Australia Council for International Development (ACFID).	These guidelines assist Australian Council for International Development (ACFID) members and their partners to understand and apply principles of ethical research conduct. They are an educative tool to support and advance ethical research.
DFID (2011) <i>DFID Ethics Principles for Research and Evaluation</i> . United Kingdom: Department for International Development (DFID).	The UK Department for International Development's principles on ethical practice in research and evaluation (ethics policy).
European Commission (2016) <i>Guidance note – Research on refugees, asylum seekers &amp; migrants</i> . European Commission, Directorate-General.	This guidance note is not specific to trafficking but includes principles and guidance that can be adapted to the TIP context. It aims to support self-assessment of ethics of research involving vulnerable groups and sets out considerations on protecting personal data and guarding against misuse.
European Commission (2005) <i>The European Charter and Code for Researchers</i> . EURAXESS.	This is a set of general principles and requirements, which specifies the roles, responsibilities and entitlements of researchers as well as of employers and/or funders of researchers.
ICRC (2016) <i>Rules on Personal Data Protection</i> . Geneva: International Committee of the Red Cross (ICRC).	These rules, while not specific to trafficking data, offers 27 articles setting out principles including rights of data subjects; and commitments; data transfer; and implementation of data protection measures in the humanitarian space that can be adapted to a trafficking context.

<sup>206</sup> Easton, H. and R. Matthews (2016) 'Getting the Balance Right: The Ethics of Researching Women Trafficked for Commercial Sexual Exploitation' in Siegel, D. and R. de Wildt (Eds.) (2016) *Ethical Concerns in Research on Human Trafficking*. New York: Springer. See British Society of Criminology (2006) *Code of Ethics for Researchers in the Field of Criminology*. UK: British Society of Criminology.

<p>IOM (2010) <i>Data Protection Manual</i>. Geneva: International Organization for Migration (IOM).</p>	<p>The manual is comprised of three parts: 1) IOM data protection principles as informed by relevant international standards; 2) guidelines on each principle and 3) generic templates and checklists to ensure that data protection is taken into account when collecting and processing personal data.</p>
<p>Markham, A. and E. Buchanan (2012) <i>Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee</i>, Version 2.0. Association of Internet Researchers.</p>	<p>These recommendations draw from the day-to-day practices of researchers in a wide range of disciplines to provide a universal set of norms, principles, practices, and regulations in terms of internet research.</p>
<p>ODI (2017) <i>The Data Ethics Canvas</i>. Open Data Institute (ODI).</p>	<p>The Data Ethics Canvas helps identify potential ethics issues that may arise in data collection by taking the data collector through a series of questions on how data is collected, how data is shared and how data is used. It “promotes understanding and debate around the foundation, intention and potential impact of any piece of work, and helps identify the steps needed to act ethically”.</p>
<p>OHCHR (2016) <i>A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance Note to Data Collection and Disaggregation</i>. Geneva: Office of the United Nations High Commissioner for Human Rights (OHCHR).</p>	<p>This guidance note is not specific to trafficking data, but offers relevant principles, recommendations and good practices in relation to participation; data disaggregation and collection by population group; self-identification; transparency; privacy and accountability.</p>
<p>RCUK (2013) <i>RCUK Policy and Guidelines on Governance of Good Research Conduct</i>. UK: Research Councils UK</p>	<p>The Research Councils UK Policy and Guidelines on the Governance of Good Research Conduct aims to help researchers and research organizations apply the highest standards to their research.</p>
<p>Schenk, K. and J. Williamson (2005) <i>Ethical Approaches to Gathering Information from Children and Adolescents in International Settings: Guidelines and Resources</i>. Washington, D.C.: Population Council.</p>	<p>These guidelines are not specific to trafficking, but to children and adolescents including those who have experienced trafficking. They contain key considerations and practical questions to guide ethical assessments, as well as recommendations and sample documents.</p>
<p>WHO (2011) <i>Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants</i>. Geneva: World Health Organization.</p>	<p>This document is intended to provide guidance to research ethics committees on which organizations rely to review and oversee the ethical aspects of research, as well as to the researchers who design and carry out health research studies.</p>
<p>United Nations (2015) ‘Professional Ethics’, <i>United Nations Fundamental Principles of Official Statistics: Implementation Guidelines</i>. Geneva: United Nations.</p>	<p>The implementation guidelines for “Professional Ethics” list several actions or activities, which a statistical agency is advised to take into account when aiming to improve the practical and effective implementation (or development of) professional standards and ethics.</p>

Relying on existing, publicly available policies and guidelines avoids unnecessary duplication of effort. As one UN researcher noted:

...we share quite regularly the UNIAP ethical research guidelines, which I think are a pretty solid statement of ethical considerations with respect to attempting to do TIP research ... We just pretty much follow the basics in terms of data collection, in terms of...anonymity and confidentiality and being mindful of cultural norms when the data is being collected, etcetera. We haven't actually developed our own ethical guidelines.

Self-administered tools and guidelines may advance high ethical standards and be even more cognizant of the ethical risks associated with TIP data collection. However, the robustness of these self-administered tools and guidelines requires that they be applied in practice. 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.

Internal ethical research and data collection policies can be instrumental in addressing those risks, as can mechanisms of oversight. Several organizations require that particular policies be applied in the design and implementation of all data collection activities and may even have a system of oversight in place, with designated consequences for deviations from those policies. For instance, IOM's *Data Protection Manual* requires an independent body to oversee implementation of the principles and investigate any complaints and specify that measures will be taken to remedy and breaches of rights and interests of data subjects.<sup>207</sup> Another example is UNHCR's *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, which sets out principles, rights of data subjects and data protection measures that are mandatory for all UNHCR staff.<sup>208</sup>

Many organizations adhere to Codes of Conduct that are either specific to their organization or are of wider application to a field or profession. Some may relate to conduct of employees broadly or may be specific to research.<sup>209</sup> Some are offered by funders of research to set out minimum standards (including ethical standards) that must be met in any research they fund.<sup>210</sup> The extent to which such Codes of Conduct are effective varies by context. However, having a Code of Conduct in place in the absence of other mechanisms of ethical review and oversight is advisable.

Finally, there have been recent efforts to develop ethical guidelines and standards in data collection that involves Big Data. As existing ethical frameworks were not drafted in anticipation of such large-scale, high-tech research strategies, many organizations are now developing self-administered Codes of Conduct. Current efforts to develop self-administered

---

<sup>207</sup> IOM (2010) *IOM Data Protection Manual*, Geneva, Switzerland: International Organization for Migration, Principle 12, p. 97.

<sup>208</sup> UNHCR (2015) *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*. Geneva, Switzerland: United Nations High Commissioner for Refugees. The policy was developed in accordance with the UN's Guidelines for the Regulation of Computerized Persons Data Files. UNHCR's "persons of concern" include refugees, asylum seekers, stateless persons, internally displaced persons and returnees.

<sup>209</sup> Examples of Codes of Conduct that are not specific to research include but are by no means limited to: IFCR (1995) *Code of Conduct*. Council of Delegates of the Red Cross and Red Crescent; Transparency International (2001) *A Statement of Vision, Values and Guiding Principles for Transparency International*. Transparency International; and WANGO (2004) *Code of Ethics & Conduct for NGOs*. World Association of Non-Governmental Organizations.

<sup>210</sup> ACFID (2016) *Principles and Guidelines for ethical research and evaluation in development*. Australia Council for International Development; DFID (2011) *DFID Ethics Principles for Research and Evaluation*. United Kingdom: United Kingdom Department for International Development; EC (2005) *The European Charter and Code for Researchers*. Brussels, Belgium: European Commission; RCUK (2013) *RCUK Policy and Guidelines on Governance of Good Research Conduct*. United Kingdom: Research Councils UK; and UKRIO (2009) *Code of Practice for Research*. United Kingdom: UK Research Integrity Office.

guidelines and standards for ethics in Big Data are included in Table #6: *Guidelines on the ethical collection of TIP data*, above, which is a non-exhaustive list intended as a resource on guidelines for ethical data collection.



## 6.4 Peer review processes

Peer review is considered to be fundamental in assuring research quality. It also offers a useful mechanism in assuring ethics in various ways. As noted in the UK Research Integrity Office *Code of Practice for Research*:

Organizations and researchers should be aware that peer review is an important part of good practice in: the publication and dissemination of research and research findings; the assessment of applications for research grants; and in the ethics review of research projects...While carrying out peer review, researchers may become aware of possible misconduct, such as plagiarism, fabrication or falsification or have ethical concerns about the design or conduct of the research.<sup>211</sup>

Nonetheless, the approach has also been questioned in terms of subjectivity, with concerns raised that it is inconsistent and biased, not always effective or efficient, slow and cumbersome. The application of peer review procedures is also very uneven from project to project and in different settings. As noted by the UK Research Information Network:

The principle that judgments should be made by experts who are respected in the field – peer review – is held by most researchers to be fundamental to any effective system for assuring or assessing research quality. Peer review attracts deep and strong support across the research community. But it comes in a number of different forms, and practices vary considerably in different contexts and fields. Peer review also attracts criticism, on the grounds that it brings delay; that it is not always effective in detecting misconduct and malpractice; that the selection of reviewers may introduce bias into the system; that the judgments made are subjective and inconsistent; that it tends toward conservatism and stifles innovation; and that it disadvantages interdisciplinary research. There are also concerns about the costs of the system (which are largely hidden, since peer reviewers are generally not paid for their time); that the burdens being placed on the reviewing community may become unsustainable as the volumes of research activity and publications continue to increase; and that there is a need for more training of reviewers to ensure greater consistency.<sup>212</sup>

Generally, peer review processes are used by academic journals and books to ensure that published research is of an adequate standard. Peer review procedures are also used by some organizations to bring a critical lens to a study or data collection project. Some organizations voluntarily subject their research and data collection to peer review as a means of augmenting the quality of the work, 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 generally advantageous to the overall outcome. It does, however, require time be allocated for review, the willingness of peer reviewers to participate in what is generally a voluntary and time-consuming review process and the time, resources and commitment of researchers to make the needed revisions and adjustments based on peer review, which may sometimes be substantial.

---

<sup>211</sup> UKRIO (2009) '3.14 Peer Review', *Code of Practice for Research*. United Kingdom: UK Research Integrity Office.

<sup>212</sup> RIN (2010) *Quality assurance and assessment of scholarly research: A guide for researchers, academic administrators and librarians*. United Kingdom: Research Information Network, p. 8.

Peer review mechanisms may include informal review by a group of relevant peers or may involve a mechanism of internal review within the organization. Peer review can be used to offer ethical oversight in 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. Another variation of peer review involves including data collectors in reviewing and validating the research results. This approach, used by one NGO in Asia when conducting its research, offers important checks and balances on research results including more accurate findings, as the NGO director explained:

Sometimes we are on another tangent [in the analysis] and their [data collectors] clarity, coming from the people who actually did [the data collection] was so necessary.

Yet another version of peer review might involve respondents from a particular project reviewing the findings or outcomes of 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 feedback as well as giving some consideration to compensation.

Regardless of the approach, peer review does offer an important check on research, including ethical issues, and could be used to a greater extent in the field of TIP data collection. The usefulness of peer review or advisory mechanisms has also been highlighted by the Australian Council for International Development (ACFID) in its *Principles and Guidelines for Ethical Research and Evaluation in Development*: “Establishing an advisory or peer review group of individuals with expertise in the research area and/or methodology is a useful process for advice on how to address ethical issues throughout the research”.<sup>213</sup> At the same time, the ACFID also notes that such a group should not replace ethics review or ethical protocols but rather is a helpful support mechanism.



## 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 sources and subjects). An example of the involvement of a third-party that is incidental to data collection is when 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 the absence of dedicated ethics oversight, this mechanism ought to protect the specific interests of a specific subject of data collection.

In some cases, an individual is afforded protection not because they are the subject of data collection but on the basis of another status. However, the other status (for instance, a child

---

<sup>213</sup> ACFID (2016) *Principles and Guidelines for ethical research and evaluation in development*. Australia: Australia Council for International Development, p.19.

who has had a guardian appointed because they are a victim of trafficking or an unaccompanied migrant) may signify that the individual is particularly vulnerable, which may be the reason that they are a relevant research participant, but also necessitates a rigorous form of ethical review. Further, the extent to which individual guardians or protection institutions have capacity to identify and mitigate ethical risks of data collection will vary significantly. Indeed, many guardians will have no expertise or experience in either research and data collection or in ethics. Their capacity and commitment as guardians is also uneven.

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 research participants. This approach can take many forms, depending on the context. It could involve consultation with community leaders who are in contact with the target population of a given study. It could also involve contacting possible respondents through NGOs or state services providers already working with them, to clearly explain the research/data collection and assist them in making an informed choice about whether or not to participate. In this way, risks may be identified and addressed if gatekeepers are involved in decisions around participation in data collection and, in some cases, limit or deny access to target populations.

In involving a third-party to recruit research participants, when gatekeepers (who may not be well-versed in ethics) prioritize their recruitment over protection considerations, meaningful consent of data collection subjects is likely to be compromised. Consent is also compromised when the consent of the gatekeeper is accepted in lieu of the consent of the research participants. One researcher described this challenge in conducting data collection with trafficked children:

I prepared this protocol whereby someone identified as a child protection gatekeeper was to read a letter that explained everything about the [research] process, what kind of questions would be asked, what their rights were, confidentiality and anonymity, the rules in terms of what would happen to the data, who would be listening, the recording, the only people who would be listening to that, how long we had to keep the raw data before we destroyed it, giving them all the information. And then I had asked for this child protection gatekeeper to do the same thing ahead of my coming there [to conduct interviews] ... However, that didn't happen systematically. So there were cases where children didn't even know they were going to be interviewed.

Other issues arise when gatekeepers have a poor understanding of research or a fundamental mistrust of researchers, so as to preclude access to potential research participants for reasons unrelated to their well-being. There can also be a problem when gatekeepers do not thoroughly consider the nuances of the research before automatically declining access to participants. One researcher reflected on additional ethical challenges in working with gatekeepers to conduct data collection with children:

...working through gatekeepers has its benefits, but also has its downsides. Because often you're relying on gatekeepers to tell you which children are ready or which children should take part [in data collection]. And I think not having the understanding of the background or not really understanding how these decisions are made is quite difficult [as a researcher]. Another issue...is when you're doing a piece of research and you observe the situation that children or young people are living in and they're in a protective space or facility and you observe really bad practice, or they tell you something about what is happening where they are. I think dealing with those issues, when [the] child protection coordinator is someone who is based at the organization, but there is an issue that the child reports about that organization, for example, is really tricky. ...that needs to be thought through before – how you deal



with those types of issues. Because if a child discloses something to do with abuse or violence, which was happening outside, then obviously you work through that gatekeeper around how you deal with that disclosure. But if it's to do with the space where [the child is], to do with that organization, then that becomes really tricky and complex.

In other cases, third-party engagement may involve government officials or law enforcement who serve as gatekeepers to detained persons. In still other cases, private sector actors may serve as gatekeepers, such as when employers allow data to be gathered on or from employees in their supply chains.

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 ethics principles for research 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 TIP 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 TIP.

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 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). Some TIP data collection involves human subjects, which raises specific ethical considerations as to how that data is collected and processed. The ethical implications of these variations of TIP data collection must be carefully considered and addressed.

Different approaches have been taken to ensure ethical TIP data collection. Ethics review bodies and Institutional Review Boards (IRBs) offer safeguards for research subjects. However, there are also limitations to ethics review in some TIP 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 situations when research and data collection are carried out in partnership with government ministries involved in the anti-trafficking response in the country or with academic institutions that have mechanisms for ethical oversight in place. Partnerships can offer significant benefits, primarily by linking research and ethics expertise with trafficking expertise, but do not automatically 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 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 the organization. Peer review can be used to offer ethical oversight in the design and implementation of data collection projects and its use and dissemination. One variation of peer review involves including data collectors in reviewing and validating the research results. Another version of peer review might involve research participants 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 participants. An example of the former is when children are enrolled in state child protection systems and have an appointed guardian safeguarding their best interests as a gatekeeper in data collection.

Ethical principles should underpin all TIP data collection activities, whether involving research or administrative data. Ethical issues arise at each of the stages of data collection process and may change over time. As appetite for human trafficking data increases and is collected 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 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. As the collection of administrative and other types data is incentivized through the prospect of funding, without parallel systems of ethical oversight being developed alongside it, there is a growing risk that data will be collected, disseminated and used unethically and potentially dangerously. As technologies rapidly advance, capacity to collect data – and the risks associated with doing so – evolve in complex and unpredictable ways. The following sections address some of these issues, with respect to: information communications technology (ICT) and third-party technology providers; using Big Data in anti-trafficking work; using Open Data in anti-trafficking work; and private sector engagement in anti-trafficking.

These sections are not mutually exclusive but rather overlap and intersect. 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.

### Emerging issues in TIP data collection

- Information communications technology and third-party technology providers
- Using Big Data in anti-trafficking work
- Using Open Data in anti-trafficking work
- Private sector engagement in anti-trafficking

### Definition. Information communications technology (ICT)<sup>214</sup>

Information communications technology (ICT) refers to technologies that provide access to information through telecommunications. ICT includes the internet, wireless networks, cell phones and other communication mediums. ICT has no universal definition; the concepts, methods and applications involved in ICT are constantly evolving. That being said, ICT essentially covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form – for example, personal computers, digital television, email and robots.

---

<sup>214</sup> Tech Terms (2017) 'ICT Definition', Tech Terms. See also, for example, Khatkar, V. (2011) 'Information and Communication Technology in Furtherance of Governance - Some Use Cases', *International Journal of Computing and Business Research*, 2(3).



## 7.1 Information communications technology and third-party technology providers

Increasingly, TIP data collectors and anti-trafficking actors are working to leverage ICT to enhance TIP data collection.<sup>215</sup> Many forms of TIP data collection are increasingly being supported by new technologies as well as the engagement of third-party technology providers. And 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 such cases, ethical and legal questions arise, including about data ownership (these questions may be amplified in the context of Big Data, discussed further in Section 7.2 *Using Big Data in anti-trafficking work*). There are also issues of data security, while, at the same time, many benefits offered by ICT. As one researcher noted:

Obviously you need to build in the safety and encryption that protects it from hacking...we've seen in just the last year or so the real risks involved with that...paper and pen has its own risks, but the fact that you used an electronic format doesn't necessarily mean everything is safer. In fact, it could be [if] somebody hacks in or a phone or a device that has a lot of data is lost or stolen or seized, you could be looking at other risks.

In short, the use of ICT raises many and varying legal and ethical issues with respect to discussions around TIP data collection. These relate to data ownership in the context of ICT, data sharing with third-party technology providers, reliance on third-party technology providers and the anti-trafficking responsibilities of ICT providers, each of which is discussed in turn below.

### Issues in information communications technology and third-party technology providers

- Data ownership in the context of ICT
- Data sharing with third-party technology providers
- Reliance on third-party technology providers
- Anti-trafficking responsibilities of third-party technology providers

### 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 human trafficking 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. For instance, when the state funds data collection and use, can the government demand access to the data collected? Even when a state is not funding a data collection activity, there may be grounds upon which the state can demand access to data or otherwise interfere with its collection and use.

Partnerships and the commensurate outsourcing of responsibilities layer additional data ownership questions on top of already difficult data protection issues. Roles and

---

<sup>215</sup> See, for example, Gerry, F., J. Muraszewicz and N. Vavoula (2016) 'The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns', *Computer Law & Security Review*, 32, pp. 205-217.

responsibilities of different partners may trigger competing claims of data ownership and have bearing on the requirements, norms and standards that come into play. Professional norms and ethical requirements may be involved when data collecting partners are academic or may be entirely absent when private enterprises are involved. Some TIP-relevant data may fall within the purview of non-disclosure agreements that commercial actors have entered into. Different constellations of actors will raise different standards of practice for data collection as well as questions about data ownership.

In 2017, NGO World Vision International (WVI) published a discussion paper on data protection, privacy and security for humanitarian and development programs that considered the risks posed by ICT being utilized by international and local NGOs, civil society actors, UN agencies, donor agencies and private sector companies to capture, analyze and leverage data about beneficiaries and sub-populations. Based on its research, WVI advised that new technology in the information management space may revolutionize how data is collected, how it serves beneficiaries and that its potential utility and risks must be understood accordingly. WVI raised issues surrounding data ownership noting that, at present, it is not practically possible for a beneficiary to request to see all the data that has been collected about them, find out with whom it has been shared and/or ask for it to be deleted, concluding that “a more organizational and industry change will have to occur before this becomes a reality.”<sup>216</sup> The same is true in the anti-trafficking context.

**Box #8. Questions about data ownership when internet platforms host data**<sup>217</sup>

Salesforce, a cloud-computing platform, was designed as a commercial tool and is now being adapted for TIP data collection, including case management data about trafficking victims. The use of cloud-computing platforms for TIP data collection may bring several jurisdictions into play including the country where the company that owns and offers Salesforce is registered, the different countries where data may be entered into the platform, and the jurisdictions where data may be stored (across several servers globally) as well as accessed and analyzed.

Questions about data ownership also arise when internet platforms are involved in hosting data, particularly when multiple sources from multiple jurisdictions have been used to source that data, as illustrated in the example in Box #8.<sup>218</sup> 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 around 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. For instance, the pervasiveness of digital recording options has made human subjects research that captures visual and/or vocal identity readily available and instantaneously shareable. As one United States university IRB has stated:

<sup>216</sup> World Vision (2017) *Discussion Paper: Data Protection, Privacy and Security for Humanitarian & Development Programs*. Federal Way, United States: World Vision International, pp. 12-14.

<sup>217</sup> Rodriguez, G. and A. Patel (2016) *Life after Salesforce*. Medford, United States: Tufts University.

<sup>218</sup> ICT providers (such as Facebook and other social media platforms) often house physical data centers on plots of land in different jurisdictions in the U.S. and elsewhere in the world. Data Center Knowledge (2010) ‘The Facebook Data Center FAQ’, *Data Center Knowledge*.

The rapidly-diversifying means for both recording and disseminating such materials makes this arena of human subjects work all the more complex. Such participants are not fictional characters, but people whose rights to privacy, informed consent, and fair representation are in the hands of a researcher or media maker. It is the researcher's/media maker's responsibility to think through the potential risks to subjects.<sup>219</sup>

There are complexities involved in the rules that should apply to govern the sharing of data in the context of ICT, including which laws apply to an NGO sharing data within the organization or with an NGO in another city or country. When sharing data externally, a degree of control can be maintained by limiting what is shared and how it is shared.<sup>220</sup> Further guidance should be developed regarding data sharing between agencies and across borders and adapted to a given country context.<sup>221</sup>

#### **Box #9. New capacities to share data utilized in anti-trafficking work**

Blockchain, originally developed to run “cryptocurrencies” like Bitcoin, is a decentralized database that is shared among a network of computers. All computers in the network must approve an exchange before it can be recorded in the database, eliminating the need for a trusted intermediary (for example, a currency exchange or bank) because the information is held securely and transparently for all users on the network to see. Microsoft is working with partners on a secure identity system that uses Blockchain to independently verify people’s identities.<sup>222</sup> Blockchain is also being used by civil society groups to make supply chains transparent (for example, through worker identification and remote monitoring of working conditions).<sup>223</sup>

Additional and complex issues emerge in determining what approaches should be taken in data sharing via cloud-computing platforms that can make data instantaneously available across jurisdictions. Here it should be noted that the EU’s GDPR imposes restrictions on the transfer of personal data outside of the EU and requires that the organization receiving the data provide adequate safeguards to ensure an individual’s rights are legally enforceable and that effective legal remedies are in place for individuals following the transfer.<sup>224</sup>

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).

When contracts clarify that the organization (for example, an NGO) that enters the data remains the data owner, rather than the database provider, questions may still remain about what the database provider can do, if anything, about unethical data being entered into those databases. There is a risk that confusion over ownership will result in defaulting to the lowest standard of protection. Or, in light of the fact that protection frameworks have not

<sup>219</sup> HSRRC (2017) *Guidelines for Media Projects Involving Human Subjects*. Los Angeles, United States: Occidental College, Human Subjects Research Review Committee.

<sup>220</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment*. Responsible Data Forum, pp. 84-85.

<sup>221</sup> World Vision (2017) Discussion Paper: Data Protection, Privacy and Security for Humanitarian & Development Programs. Federal Way, United States: World Vision International, p. 11.

<sup>222</sup> Hutt, R. (2016) ‘Beyond bitcoin: 4 surprising uses for blockchain’, *World Economic Forum*, December 13.

<sup>223</sup> Capri, A. (2018) ‘How Blockchain Could Help End Modern Day Slavery in Asia’s Exploitative Seafood Industry’, *Forbes*, February 18.

<sup>224</sup> EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union (“General Data Protection Regulation” or “GDPR”), Article 45 and Recitals 103-107 and 169.

caught up with data collection capacities, there may simply be an absence of applicable standards.

In practical terms, it is ultimately the actor that has the capacity to share data who decides 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. In the commercial sector, some regulations have been developed to strengthen protection of data that is shared across borders.<sup>225</sup> Would such regulations also apply to commercial actors who are acting outside of the commercial context?

**Box #10. Self-determined criteria for data protection in the private sector<sup>226</sup>**

Facebook, the well-known U.S. social media service company that utilizes ICT, shares data with other companies, including third-party partners and customers. In some cases, Facebook shares user data even after a user has deleted their account. Facebook may also “access, preserve and share” information in response to legal requests such as search warrants, court orders or subpoenas, if it has a “good faith belief that the law requires [Facebook] to do so”. Facebook also explains to its users that it may also access, process and retain information about them for an extended period of time in response to a legal request or obligation or investigation. These self-determined criteria show the wide discretion that Facebook, a for-profit private enterprise, exercises in responding to legal requests. In recent years, Facebook was criticized for sharing data with researchers without obtaining informed consent from the individuals whose data was shared.

Facebook recently acquired the application WhatsApp, an encrypted instant messaging service used by over one billion people globally. While Facebook initially stated that it would keep user information for the two services separate, it subsequently announced controversial data sharing plans, which were suspended by the European Commission in November 2016. In May 2017, Facebook was heavily fined by the EU for providing misleading information about its takeover of WhatsApp.

The capacity to share data is increasingly resting in the hands of private sector actors. Questions arise around the unintended negative (or even unethical) consequences of digital identity and tracking individuals using technology, that may be particularly acute in human trafficking and related fields, where the identities at issue are those of particularly vulnerable people. There is a tension between the use of this technology to provide digital identities (for example, to migrants and trafficking victims) and the lack of discussion around the ethics, legality and risks. There is also a lack of engagement with trafficking victims and migrants themselves to determine if digital identities and tracking are something they want and need (and what the positive and negative implications may be). One NGO director highlighted the need for discussion on these issues:

In trafficking, obviously, but in migration as well, you’re dealing necessarily with people who are very poor. And they have no identity footprint. And often they don’t have a passport and they may not have any bank account. They may not have any credit cards or subscriptions. In actual fact, they may not have anything that records who they are or where they’ve been. Obviously, that’s one of the challenges...[and] for someone who has no identity ... [for them, the ability to be] registered somewhere, that they are known and that they will [have an identity footprint and] continue to be [known] regardless of what happens can be important [to them]... And the law around it and the ethics around it are definitely not discussed.

<sup>225</sup> For instance, the EU-U.S. Privacy Shield allows personal data to be transferred from the EU to a company in the U.S. providing that that company uses, stores and further transfers the data according to data protection rules and safeguards. However, the Privacy Shield applies only to those companies who have signed up for it. EU (2016) ‘The EU-U.S. Privacy Shield’, *Data Protection*, July 12.

<sup>226</sup> Facebook (2017) *Data Policy*. Menlo Park: Facebook; and Gibbs, S. (2017) ‘WhatsApp faces EU taskforce over sharing user data with Facebook’, *The Guardian*, October 26.

### Box #11. Private sector actors selling data<sup>227</sup>

In April 2017, the U.S.-based startup Unroll.me (a free tool for managing subscription emails) was criticized for using data for commercial intelligence. One case study of ethical concerns noted: “Users allow Unroll.me to access their emails and email histories as part of Unroll.me’s service...[Unroll.me then] sells anonymized email data from [users] to businesses looking for insight into the services people access and their purchasing habits. Despite agreeing to Unroll.me’s terms and conditions...Unroll.me users and potential users were seemingly unaware that their email histories were being monetized [and] sold...While the purposes for which Unroll.me used their customer data were outlined in their terms of service agreement, this did not alter the perception that their behavior was unethical”.

Issues emerge not only in the context of how data is shared but also relating to the ramifications of sharing for the individuals about whom the data pertains. Alongside these considerations is whether, as the capacity to wield this data is increasingly in the hands of private sector actors, private sectors are equipped and concerned with adequately protecting the interests of vulnerable persons. More generally (and as noted above), a recent study on data sharing to third-parties by mobile applications (apps) found that a significant proportion of apps share data from user inputs with third-parties, including personal information and search terms without requiring a notification to the user.<sup>228</sup>

While the examples in Box #10 above and Box #11 are not specific to trafficking in persons, they are increasingly meaningful in light of growing efforts by anti-trafficking actors to identify and embrace technological approaches to confront human trafficking. While technological and other innovative approaches offer some new and promising strategies that should be examined, the contours of issue-sharing must be part of the equation. These examples highlight the self-determined criteria and extreme discretion used by private sector actors in terms of data sharing, which should raise alarm bells for anti-trafficking actors seeking to mobilize such technology solutions. Organizations and institutions need to carefully consider how their sharing and use of data may be perceived, even when it is technically legal, as that can help to navigate the boundaries between ethical and unethical data collection practices.<sup>229</sup> Apart from purely ethical considerations, anti-trafficking organizations have not yet had to respond to the type of potential reputational risk that these examples suggest commercial enterprises have already faced.

### 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 the capacity of users to protect data. For instance, when a technology company develops a technology-based method of data collection and provides (or sells) that method to data collectors, it is important to consider whether the user (potentially a service provider, police officer, social scientist) has capacity to use that technology in a way that adequately protects privacy. Other questions to consider include: What are the implications for data (and the interventions based on it) when an NGO or government agency is unable to collect,

#### Questions about technology-based methods of data collection

- ② Does the data collector have the capacity to use the technology in a way that protects privacy?
- ② What are the implications when data collector cannot collect, enter and store data safely and correctly?
- ② When accessing existing datasets, how is consent dealt with?

<sup>227</sup> Broad, E., A. Smith and P. Wells (2017) *Helping organisations navigate ethical concerns in their data practices*. United Kingdom: Open Data Institute, p. 24.

<sup>228</sup> Zang, J. et al. (2015) ‘Who Knows What About Me? A Surevy of Behind the Scenes Personal Data Sharing to Third-parties by Mobile Apps’, *Technology Science*.

<sup>229</sup> Broad, E., A. Smith and P. Wells (2017) *Helping organisations navigate ethical concerns in their data practices*. United Kingdom: Open Data Institute, p. 25.



enter and store data safely and correctly? Where databases are fed by or draw on datasets that may be several years old, is it relevant that individual data sources did not consent to it being shared and used for purposes other than those for which they originally consented to provide it?

One program manager for a TIP data collection project described the on-the-ground challenges of implementing a technology-based solution to data collection, where caseworkers were provided with mobile phones to collect case data on identified trafficking victims, which was then to be transmitted into a shared database:

We had an application that we developed in house that caseworkers could use on phones and that we procured and distributed through the project. They could fill out these forms and then refer those cases. That data could be collected centrally and then accessed by caseworkers who were assigned the respective cases. ... we trained all of the caseworkers on the use of the forms and the use of the phones to fill out the forms. And we did several follow-up trainings as well. But we had challenges with access to internet and the basic capacity [of social workers] to use the phones for the purposes of filling out the forms. We had caseworkers who had never used a computer before. And we were asking them to fill in forms on a little smart phone, which was not realistic. And it quickly became clear that we either had to provide a lot more training and a lot more capacity building or somehow figure out a way to do paper forms in addition or to complement the online forms. And we also had issues with the retention of NGO staff. There was a lot of turnover among some of the NGOs that we were working with and we lost a lot of the phones. Or they broke. And we had to replace them... at a practical level it was a challenge.

One study noted the need for “translation” in many partnerships, with human rights not understood by the technology partner or technology not understood by the human rights partner. That is:

To understand how cutting edge technological innovation can be applied in the human rights and security arenas often requires cross disciplinary “translation” work. Human rights experts may not have the vocabulary to convey their “asks” to engineers or statisticians. Similarly, software developers may know little about consequences to vulnerable populations. A translator or broker is often needed for diverse actors to establish a baseline understanding around data, evaluate the efficacy of emerging technologies and develop actionable strategies.<sup>230</sup>

This observation has relevance also in the anti-trafficking field, where many organizations and institutions described a disconnect between themselves as subject matter experts and technology providers.

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 advantages and disadvantages 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

---

<sup>230</sup> Latonero, M. and Z. Gold (2015) *Data, Human Rights & Human Security*. United States: Data & Society Research Institute.

can access it and for what purpose.<sup>231</sup> In jurisdictions where digital files and downloaded materials may be subject to subpoena, it may be advisable for non-state actors to limit what data (particularly personal and sensitive data) is digitally stored.<sup>232</sup> On the other hand, in some jurisdictions cloud-based data may not be obtainable through subpoena (because it is not stored in the jurisdiction), raising questions about what data should or should not be obtainable, for instance, when it can serve victim or perpetrator identification.

When anti-trafficking actors partner with technology providers, the encroachment of the private, commercial sector into anti-trafficking work also raises complex questions about the ethics of “profiting” from such endeavors.

This monetization, or adding a commercial value to data, can potentially have negative ethical consequences. For instance, although it may be legal for a private enterprise to purchase data from an anti-trafficking NGO, this activity may pose serious ethical risks by compromising data protection and protection of data subjects, particularly where NGOs are underfunded and may need the income to continue their work. On the other hand, when such technology is provided for free, is the result that the provider becomes a “partner” in the project and, as such, retains a claim of ownership on the data that it collects? Additional questions include: when a private-sector actor has data or the means of contributing to trafficking prevention, should they be able to profit from putting that data into the hands of those who need it for this work? Or should they be required to “give back” to the countries and communities they profit from, and if so, on what legal, ethical or other basis?<sup>233</sup>

#### Questions about partnerships with technology providers

- ② Is it ethical to fund for-profit private sector stakeholders assisting in TIP data collection?
- ② What are the implications of adding a commercial value to TIP data?
- ② What questions of TIP data ownership arise?
- ② Where is there an ethical obligation to share TIP data?

Another concern raised by dependence on third-party software and technology-platform suppliers, is the increased cost associated with paying for their services. International and/or well-funded actors may have greater access to such services and the partnerships that use them, to the disadvantage of smaller-scale, lower-resourced civil society actors. In the long-term, the result may be to increase the cost of anti-trafficking work more generally, which may have a negative impact on direct service provision to victims and vulnerable populations, many of whom are supported by smaller and less funded NGOs. Furthermore, the quality of data and its ethical use may decrease over time as particular for-profit technology providers achieve a monopoly over the marketplace and subsequently attain power to dictate the ethical framework involved, whether to lower the standard or raise it. Such a monopoly also raises questions as to the extent that such providers own the data – if not in law, then in fact – and can accordingly make decisions as to what to do with it.<sup>234</sup>

<sup>231</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Department*. Responsible Data Forum, pp. 39-41. In this context, though, it is also important to note that the GDPR applies to both data processor and controllers, meaning that clouds are not exempt. EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union (“General Data Protection Regulation” or “GDPR”).

<sup>232</sup> Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Department*. Responsible Data Forum, p. 48.

<sup>233</sup> Schlanger, Z. (2017) ‘The UN wants Facebook to fix its human trafficking problem’, *Quartz*, September 28.

<sup>234</sup> Broad, E., A. Smith and P. Wells (2017) *Helping organisations navigate ethical concerns in their data practices*. United Kingdom: Open Data Institute, p. 22, noting: “Unfair monopolies can arise where data access is restricted to one organisation or a small number of organisations, where it might otherwise reasonably be shared”.

Other challenges emerge when those who depend on third-party, for-profit technology suppliers are not NGOs or international organizations but state actors. As new technology evolves to combat serious crimes like trafficking in persons and the private sector's capacity to design technological solutions outstrips the states' capacity to do so, state law enforcement authorities are increasingly reliant on private sector actors, including in the realm of intelligence data. Recent technology-driven initiatives reveal that non-state data collection providers are increasingly encroaching on criminal justice intelligence space.<sup>235</sup> Some private technology entities even have digital crimes units that essentially "police" the internet through high-tech surveillance and analytics, to identify potential victims of trafficking and potential traffickers. One project manager described some of these activities:

A lot of it also has to do with tracking people across borders, which becomes a bit of a law enforcement thing... Using web crawling technology to search for sites that are recruiting people, the ones that pop up for two weeks and then disappear... Getting in and disrupting the sites are things that are possible to do now. And then there are other kinds of technologies that we can use to identify and actually geo-locate people based on who is using social media against key word searches. [...] where you're interested in trying to identify where "bad guys" are operating, particularly on the internet, there's different technologies that can search the web based on key words...it's open-source intelligence, which is basically a surveillance technology. The computer basically does all the work for you, it constantly scans the internet to find sites or activity that may be on social media or some other online activity where it will identify where the hits that the key words make. It will tell you what the frequency is, what the volume is, what the location is, et cetera and it can do it really fancy geo-mapping types of things that can actually even identify where a site is hosted. And this is crawling in the deep web too.

When non-state actors host such data, issues emerge as to who owns, has access to and/or can share what is essentially law enforcement intelligence data. Further questions arise regarding the relationship between non-state technology actors and state law enforcement actors and what, if any, framework of laws or regulations may exist to govern that relationship. Questions also arise as to when information must be disclosed to authorities (for instance, evidence of crimes, including data in the form of child abuse images) and when authorities may have the ability to subpoena such information. It may also be unclear what, if any, frameworks exist to limit third-party private actors from revealing information about alleged victims or abuses, particularly when such allegations have not been confirmed through expert investigations and prosecutions. Whether sensitive or personal information is shared ultimately depends on the organization that holds it, the presence of local laws on these issues and the organization's compliance with them. The result is inconsistent protections of privacy across the globe. There is also the higher order question as to whether capacity to take certain actions against criminal phenomena such as investigation of and data collection on the organized crime of trafficking in persons, should translate into an entitlement to do so.

#### **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. Platforms such as Telegram, Threema, Twitter, WhatsApp and Facebook have reportedly been used to recruit victims into various forms of exploitation, including radicalized youth into terrorism, false job advertisements that lead to forced labor, the buying and selling of victims for sexual

---

<sup>235</sup> See, for example, the Global Emancipation Network, discussed in Section 7.2 *Using Big Data in anti-trafficking work*.

exploitation and false promises that look like opportunities to be smuggled but that devolve into situations of torture and exploitation.<sup>236</sup> This raises questions about the extent to which private sector actors have a responsibility to prevent their services from being used for criminal ends or, beyond this, to actively work with other actors (potentially including state authorities) to convert this technology into that which can instead prevent trafficking. And what are the human rights implications if these actors not only have a responsibility to support the state to fight trafficking, but also other crimes as defined by the state, such as political dissent, or forms of expression such as blasphemy?

There are examples of ICT providers using their capacities to address criminal issues connected to trafficking, such as by removing harmful data posted by users.<sup>237</sup> In the context of migrant smuggling, which may develop into situations of human trafficking, organizations have called for social media platforms to provide free advertising to raise awareness of trafficking risk.<sup>238</sup> There has been criticism that some providers are too slow to remove content, and fail to take full responsibility for the negative role they play in supporting criminal activities. Often pages are not automatically detected for removal but require individuals to report where pages should be removed. There is also concern that removing such data serves to remove crucial evidence of human rights abuses, including human trafficking, which may be used to bring perpetrators to justice.<sup>239</sup> Moreover, in the case of complex crimes like human trafficking, where content online may not appear on its surface to be criminal in nature, determining what is harmful is not straightforward. These issues, in turn, raise higher order questions relating to freedom of speech and freedom of information, and who is to determine what should be protected and what curtailed.



## 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. One example of a recent effort is detailed in Box #12 below. The key emerging challenge is to ensure that Big Data is responsible and does no harm. One researcher who studies Big Data notes that longstanding protections around vulnerable persons are not always foreseen in the world of Big Data:

Perhaps the biggest issue is that in our Big Data world, disciplinary boundaries are breaking down and fields with long histories of ethical review are being inundated with work from fields with no history of review and indeed active movements against such requirements. Data scientists are becoming a universal discipline, applying their

---

<sup>236</sup> UN Secretary-General (2016) 'Annex: Special Report of the Office of the Special Representative of the Secretary-General on Sexual Violence in Conflict', *Letter to the President of the Security Council*, 21 December 2016, UN Doc S/2016/1090; Cockayne, J. and S. Walker (2016) *Fighting human trafficking in conflict: 10 ideas for Action by the United Nations Security Council*. United States: United Nations University, p. 27; and ICMPD (2015) *Targeting Vulnerabilities: The Impact of the Syrian War and Refugee Situation on Trafficking in Persons - A Study on Syria, Turkey, Lebanon, Jordan and Iraq*. Vienna, Austria: International Centre for Migration Policy Development, p. 153.

<sup>237</sup> For instance, Google uses video analysis and independent experts to prevent violent extremism online, particularly on YouTube and even uses "redirection" to divert potential recruits towards anti-terrorism videos. Bickert, M. and B. Fishman (2017) 'Hard Questions: How We Counter Terrorism', *Facebook Newsroom*, June 15 and McVeigh, K. and M. Mahmood (2017) 'Facebook removes posts made by people smugglers aiming to lure migrants', *The Guardian*, August 25.

<sup>238</sup> Schlanger, Z. (2017) 'The UN wants Facebook to fix its human trafficking problem', *Quartz*, September 28, referring to a ransom video of an 11- or 12-year-old migrant being tortured in Libya.

<sup>239</sup> See Browne, M. (2017) 'YouTube Removes Videos Showing Atrocities in Syria', *New York Times* August 22.

methods and data across nearly every imaginable traditional domain. Just a few decades ago a documentary study of a vulnerable population in another country would traditionally be carried out by a trained ethnographer deeply steeped in human subjects research culture and informed consent and with privacy and subjects protection at the forefront of their minds. Today, that study might just as easily be conducted by a set of computer scientists who harvested millions of photographs and highly intimate personal details from afar and published a paper documenting the most private aspects of those individual's lives, or even actively manipulating their emotional well-being, without them ever knowing they were a test subject.<sup>240</sup>

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 on what data is collected and how it is captured and analyzed.

#### **Definition. Big Data<sup>241</sup>**

Big data is “extremely large datasets associated with new information technology and which can be analysed computationally to reveal possible patterns, trends and correlations.” Big Data has “three Vs”: volume (the scale of information processed), velocity (the speed at which information is processed) and variety (the wide range of types of information sources).

TIP data collection that involves Big Data raises complicated legal and ethical questions, which are discussed in the following sections, linked to the risks posed by Big Data and the need for oversight of Big Data.

### **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. As commentators from the Council on Big Data, Ethics and Society explain, Big Data “fundamentally changes our understanding of research data to be (at least in theory) infinitely connectable, indefinitely repurposable, continuously updatable and easily removed from the context of collection”.<sup>242</sup>

#### **Issues with Big Data**

- Risks posed by Big Data
- The need for oversight of Big Data

When it comes to Big Data, the relationship between researchers and data subjects becomes abstract and indistinct, which may lead to defining the research setting as excluding persons. As noted by the Association of Internet Researchers:

...the question of whether one is dealing with a human subject is different from the question about whether information is linked to individuals: Can we assume a person is wholly removed from large data pools? For example, a data set containing thousands of tweets or an aggregation of surfing behaviors collected from a bot is

<sup>240</sup> Leetaru, K. (2017) ‘Is It Too Late For Big Data Ethics?’, *Forbes*, October 16.

<sup>241</sup> OHCHR (2016) *A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance Note to Data Collection and Disaggregation*. Geneva: Office of the United Nations High Commissioner for Human Rights, p. 12 at fn 25. See also ICO (2017) *Big Data, artificial intelligence, machine learning and data protection*. United Kingdom: Information Commissioner’s Office, United Kingdom, referring to the Gartner IT Glossary. For more on this classification of Big Data and the methodologies involved, see Ellingwood, J. (2016) ‘An Introduction to Big Data Concepts and Terminology’, *Digital Ocean*, September 28.

<sup>242</sup> Metcalf, J. and K. Crawford (2016) ‘Where are the human subjects in Big Data research? The emerging ethics divide’, *Big Data & Society*.

perhaps far removed from the persons who engaged in these activities. In these scenarios, it is possible to forget that there was ever a person somewhere in the process that could be directly or indirectly impacted by the research. Yet there is considerable evidence that even anonymized datasets that contain enough personal information can result in individuals being identifiable. [...] These are important considerations because they link to the fundamental ethical principle of minimizing harm. Does the connection between one's online data and his or her physical person enable psychological, economic, or physical harm? One way of evaluating the extent to which these ethical dilemmas may be hidden is to focus on the way that procedures for data collection or analysis extract data from lived experience.<sup>243</sup>

**Box #12. Using Big Data to prevent trafficking of children<sup>244</sup>**

Operation Red Alert aims to prevent “sex trafficking” of girls in India by using Big Data for awareness-raising. Working in partnership with an Australian analytics firm Quantum (which brings together proprietary data, technology and data scientists), Red Alert analyzes census data, government education data and other sources for factors (such as drought, poverty, proximity to transportation stations, education opportunities, population and distance to police stations) to determine which of India's 600,000 villages are most at risk of human trafficking. On the basis of this analysis, mass grassroots awareness raising and education campaigns are then designed to target the villages identified as a risk of trafficking. The campaigns are implemented at the village level through network of 40 NGO partners and a national helpline is in place harnesses the ubiquity of mobile phones throughout India, to provide continual support to people in villages.

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.<sup>245</sup>

The disconnect between Big Data collection and ethical frameworks has meant that some (arguably many)<sup>246</sup> Big Data researchers do not subject their work to ethical scrutiny. Because Big Data does not directly engage with human subjects but relies on existing

data, it may be considered to be “minimum risk” and not subject to ethical review and oversight. This view is misguided given that many datasets that are harmless in their existing form can be brought together in ways that may pose risks for the individuals to whom the data relates, particularly when datasets are subject to data analytics techniques that can paint deeper and more personal pictures of individuals and communities and erode their privacy. Analytics of an individual's social media usage can effectively serve as a form of surveillance, revealing political views, immigration status, geographical position or sexual orientation. As one study notes, data collection in the digital age:

<sup>243</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 6.

<sup>244</sup> Whipple, K. (2017) ‘Big Data is reducing human trafficking in India’, *MAPR Data Technologies*, May 30.

<sup>245</sup> Crosas, M. et al. (2015) ‘Automating Open Science for Big Data’, *ANNALS of the American Academy of Political and Social Science*, 659(1); Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers; Narayanan, A. and V. Shmatikov (2008) *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*. Oakland: IEEE Symposium on Security & Privacy; and Sweeney, L. (2004) ‘Navigating Computer Science Research Through Waves of Privacy Concerns: Discussions among Computer Scientists at Carnegie Mellon University’, *ACM Computers and Society*, 34(1)

<sup>246</sup> Leetaru, K. (2017) ‘A Case Study in Big Data and the Replication Crisis’, *Forbes*, September 1; Leetaru, K. (2017) ‘AI “Gaydar” and How the Future of AI will be Exempt from Ethical Review’, *Forbes*, September 16;

Leetaru, K. (2017) ‘Is It Too Late For Big Data Ethics?’, *Forbes*, October 16; and Leetaru, K. (2016) ‘Are Research Ethics Obsolete in the Era of Big Data?’, *Forbes*, June 17.

...raises questions of whether traditional ethical frameworks that guide academic research in institutional settings and national legislative frameworks that pertain to data collection and [consent], are adequate and sufficient. In the first instance, analysis of Big Data frequently does not occur within the confines of research institutions; it is consequently not bound by human subject protections. Furthermore, Big Data is frequently collected by both public and private organizations and is therefore subject to multiple and varying international and state-based interventions and standards. Frequently, there is insufficient guidance, or practical and effective solutions to safely collect data directly or indirectly...within a digital world.<sup>247</sup>

### **Box #13. Using Big Data to tackle trafficking**

The Global Emancipation Network (GEN), a volunteer-run data analytics non-profit organization, collects data about all forms of trafficking from 22 countries across 80 jurisdictions, sourcing its data from Craigslist, Backpage and dark web sites, among others. GEN has engaged corporate partners, including Microsoft and Splunk, to use data analytics to create a searchable database to analyze trafficking data. Its goal is to become a “global clearinghouse for trafficking data worldwide” by providing a platform to host data from academia, government entities and law enforcement. GEN takes a Big Data approach pooling text, photos, images and other material to collect a “giant encyclopedia of trafficking indicators” and making it “searchable, sortable and consumable” in a bid to identify where victims might go and who may move them and to shape policy making. GEN makes its data available free of charge to users, including law enforcement, government agencies, researchers, academia and anti-trafficking non-profit organizations.<sup>248</sup>

While the disconnect between ethical standards and Big Data research extends across the spectrum of potential Big Data subjects (that is, individuals using the internet), there are specific issues when it comes to Big Data and children as data subjects. The same study notes that, to date, there has been little rigorous debate or understanding of how to adapt traditional, offline ethical standards for research, involving data collection from children, to a Big Data, online environment. This is a significant concern in a world where one in three global internet users is a child.<sup>249</sup>

Familiar ethical controls in data collection, such as informed consent, are largely absent in the use of Big Data. As one recent paper on the issue notes:

...informed consent occurs only at the point of collection. But the power and peril of data science is that data is most valuable when it can be reused and repurposed in many different contexts and in combination with other datasets. Personal and sensitive data now travels unpredictably and will be reused indefinitely for unforeseeable purposes.<sup>250</sup>

Big Data effectively allows researchers to access data about individuals – and often highly sensitive data – without having any contact with them, nor seeking their consent, nor assessing the specific risks that may arise owing to their personal circumstances or characteristics. Questions, therefore, need to be asked about the relevance, applicability and viability of traditional ethical infrastructures, principles and norms, such as informed consent and respect for persons, “when data about individuals is persistently shared,

<sup>247</sup> Berman, G. and K. Albright (2017) *Children and the Data Cycle: Rights and Ethics in a Big Data World*. UNICEF Office of Research Paper No. 2017-05. Florence, Italy: United Nations Children’s Fund, p. 2.

<sup>248</sup> See Larson, S. (2017) ‘Anti-human trafficking group uses data to track criminals’, *CNN Tech*, August 17 and Global Emancipation Network (2017) ‘Tech Strikes Against Modern-Day Slavery’, *Global Emancipation Network*, September 25.

<sup>249</sup> Berman, G. and K. Albright (2017) *Children and the Data Cycle: Rights and Ethics in a Big Data World*. UNICEF Office of Research Paper No. 2017-05. Florence, Italy: United Nations Children’s Fund, p. 1.

<sup>250</sup> Accenture (2016) *Universal principles of data ethics: 12 guidelines for developing ethics codes*. Beaverton, United States: Accenture, p. 3.

transformed, and aggregated and when future uses of datasets are so unknowable that ‘informed consent’ is a misnomer at best—and impossible at worst”.<sup>251</sup>

Similarly, questions arise as to the relevance and practical applicability of the principle of “do no harm”. That is, “does the connection between one’s online data and their physical person enable psychological, economic, or physical, harm?”<sup>252</sup> While interviewing someone face-to-face may seem substantially different (and less removed) than interviewing a person in an anonymous chatroom, a person is still involved. And as researchers have noted:

...anonymous members of online communities have felt harm after researchers published reports about what they perceived to be private community activities. Blogs are often considered public, published texts. On the other hand, users have described their blogs as a part of their identity, not to be treated as simply publicly accessible data.<sup>253</sup>

In the context of trafficking in persons, issues of irregular immigration status, irregular work, sexual behavior and other sensitive activities may be captured or revealed in datasets. Use of such data could potentially result in discriminatory or stigmatizing outcomes. Furthermore, when the individuals concerned are victims or potential victims of trafficking, the risk of identification may be serious and specific, including risks of retaliation against victims and their families by traffickers and risks of prosecution and conviction for alleged criminal activities. These risks – which data subjects have not been informed about nor consented to – have not been mitigated through ethical oversight.

Risks are exacerbated by the fact that the data yielded may be unintended at the outset. This violates the principle established across ethical and legal frameworks that only a minimum amount of data should be collected, for a limited purpose and cannot be used for any other purpose without the consent of a data subject. In Big Data, the subsequent use may well far exceed the purpose for which it was originally collected. For instance, where analytics reveals potential perpetration or unknowing support of exploitation by a set of individuals, questions arise about what to do with this data and whom to share it with.

More broadly, discussions are taking place in the humanitarian field about the risks posed by “demographically identifiable data”, which is a broader classification than personally identifiable information, and how the disclosing of and access to this “group data” could cause various harms to entire classes of people.<sup>254</sup>

As is the case with all research methods, ethical risks may also be posed by uneven representation, which is necessarily the case in the analysis of Big Data. Accordingly, the limitations of Big Data must be understood in designing interventions when the data itself has embedded biases. That is:

...big data analysis deals in possible correlations, not causation nor objectivity. Serious concerns about sampling, representation and population estimates call into question the utility of big data in policy making. Moreover, all big datasets give a biased view of reality as individuals and attributes will be excluded. New requirements for disclosing biases may be needed to alert decision makers to avoid hasty generalizations. The notion of substituting big data inferences for deep

---

<sup>251</sup> Accenture (2016) *Universal principles of data ethics: 12 guidelines for developing ethics codes*. Beaverton, United States: Accenture, p. 3.

<sup>252</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 7.

<sup>253</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 13, fn. 7.

<sup>254</sup> Karunakara, U. (2014) ‘Data Sharing in a Humanitarian Context: The Experience of Médecins Sans Frontières’ in Moore, S.A. (Ed.) *Issues in Open Research Data*. London, United Kingdom: Ubiquity Press, pp. 59-76.



expertise and judgment raises particular concerns where the consequences to human lives are paramount. Data gathered from crowdsourcing, social media, and mobile phones can give unprecedented insight for individual case analysis. But can this data used for policy making and resource allocation? Quantitative analysis from big data can provide the “scaffolding” that builds up a case. But is qualitative research ultimately necessary to verify evidence?<sup>255</sup>

## 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 enquiry, not just concerning trafficking in persons. A rising body of literature reveals that 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

### Box #14. AoIR Ethics Working Committee Fundamental Principles

- The greater the participant’s vulnerability, the greater the researcher’s obligation to protect.
- “Harm” is contextual; ethical decision-making requires the application of practical judgment attentive to the specific context.
- As all digital information involves individual persons, principles on human subjects research may be needed.
- The rights of subjects may outweigh the social benefits of research and researchers’ right to conduct research.
- Ethical issues may need to be addressed during all steps of research (planning, research conduct, publication and dissemination).
- Ethical decision-making is a deliberative process; researchers should consult as many people and resources as possible.<sup>256</sup>

methodologies, leaving uncertain whether or not they apply.<sup>257</sup> 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, as discussed elsewhere in this paper.<sup>258</sup>

Efforts to build an ethical framework should be cognizant of the on-going challenges involved in adapting biomedical science approaches to social sciences. They should build on lessons learned from experience in adapting those approaches to emerging data and computer sciences. In 2012, the Association of Internet Researchers released the document: *Ethical*

*Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*,<sup>259</sup> which makes clear that the same ethical principles that apply generally to social scientists are central in the work of internet research, which may appear, on the surface, to be more distant from some of the risks and vulnerabilities.

<sup>255</sup> Latonero, M. and Z. Gold (2015) *Data, Human Rights & Human Security*. United States: Data & Society Research Institute.

<sup>256</sup> Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 5.

<sup>257</sup> Metcalf, J. and K. Crawford (2016) ‘Where are the human subjects in Big Data research? The emerging ethics divide’, *Big Data & Society*, p. 7.

<sup>258</sup> Metcalf, J. and K. Crawford (2016) ‘Where are the human subjects in Big Data research? The emerging ethics divide’, *Big Data & Society*, pp. 1-14.

<sup>259</sup> The first version of the AoIR Ethical Decision-Making document was released in 2002, after two years of international and cross-disciplinary collaboration. The intention was to develop guidelines from the bottom up (that is, out of the day-to-day practices of researchers in a wide range of disciplines, countries and contexts, in contrast to a more usual top-down approach that tries to provide a universal set of norms, principles, practices, and regulations). This approach was crucial because the enterprise of internet research is expansive (that is, globally informed) but also situated in innumerable locales. Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers, p. 2.

The concerns raised above regarding involvement of private third-parties need also to be considered. Big Data is often generated by private entities and, as such, may not be subject to existing forms of regulated ethical scrutiny, such as ethics review. This highlights the need to import established ethical norms and principles from regulatory frameworks into emerging mechanisms that can positively impact actors involved (whether public, private or a combination of both) whose activities have the potential to raise risks of potential harms.<sup>260</sup> This means that the principles underpinning research ethics must be well understood, flexibly adapted and potentially taken outside of traditional frameworks.

An example of self-administered ethical guidance, although not related to TIP, comes from Twitter, which makes note of the sensitivity of some data types. Twitter has, since 2014, specified what it calls “sensitive categories” and prohibits the use of these categories for keyword-targeting advertisements, deeming such profiling “inappropriate or offensive” and that such use could potentially “compromis[e] users’ trust”.<sup>261</sup> Twitter also has a self-administered policy with regard to the sharing of personal data on Twitter, noting that: “Posting someone’s private information online may pose serious safety and security risks for the person whose information is shared. As such, this is considered one of the most serious violations of the Twitter Rules”.<sup>262</sup> The development and robust enforcement of ethical guidance is an important first step in regulation of Big Data use. The effective implementation of such guidance must also be ensured.

In terms of TIP data collection, it is important that stakeholders involved in Big Data (whether public or private) adapt existing frameworks to the specific concerns raised by human trafficking. As one researcher has argued:

If major funding agencies, professional societies and publishers moved to require full IRB review of all submissions (and thus disallowing IRB exemption on the basis of “publicly accessible data”) and demanding reasonable replication datasets (while adhering to relevant privacy, legal and ethical standards), then these concepts would rather quickly infuse themselves into the data sciences. While private companies would obviously still be free to conduct business as usual, the push by corporate data scientists to publish in the academic literature would mean that even major portions of their work would make its way through rudimentary review and be forced to offer at least some form of replication data. Instead of Facebook offering in the aftermath of its emotions study only that it was working on its ethical review of research, while refusing to offer any concrete detail of those changes, if journals required all authors to produce the results of full IRB review of their work, this would offer tremendous insight into the ethical reasoning of the largest data-driven companies at the forefront of Big Data research.<sup>263</sup>

Analysis is underway on the implications of the EU’s GDPR on Big Data, particularly in light of an EU Parliament resolution urging both public and private sectors to bring their Big Data practices in line with the GDPR, including by developing “concrete standards that protect

---

<sup>260</sup> Here Metcalf and Crawford raise the example of Facebook responding to public criticism of its “emotional contagion” experiment in 2014, by establishing an internal review process for external experiments. Metcalf, J. and K. Crawford (2016) ‘Where are the human subjects in Big Data research? The emerging ethics divide’, *Big Data & Society*. For more on new approaches to ethical review inside industry, see Metcalf, J., E. Keller and D. Boyd (2016) ‘Perspectives on Big Data, Ethics, and Society’, *Council for Big Data, Ethics, and Society*, May 23.

<sup>261</sup> Such categories include, for example health, negative financial status or condition, political affiliation or beliefs, racial or ethnic origin, religious or philosophical affiliation or beliefs, sex life and trade union membership. Leetaru, K. (2017) ‘A Case Study in Big Data and the Replication Crisis’, *Forbes*, September 1.

<sup>262</sup> Consequences for violation of the Twitter Rules depend on the severity of the violation and the person’s previous record of violations. Twitter (2017) ‘Private information posted on Twitter’, *General Policies*.

<sup>263</sup> Leetaru, K. (2017) ‘Is It Too Late For Big Data Ethics?’, *Forbes*, October 16.

fundamental rights and guarantees associated with the use of data processing and analytics by the private and public sector.”<sup>264</sup>

The last few years have also seen the emergence of tools and guidance on the ethics of Big Data. In 2016, the Council for Big Data, Ethics and Society released a paper outlining emerging ethical issues in data science and offering recommendations to strengthen and adapt ethical norms to the context of Big Data.<sup>265</sup> Similarly, in 2016, Accenture’s Data Ethics Research Initiative released an ethical resource for data scientists, which raises the need for a Code of Ethics to guide the profession of data science and offers a broad set of principles, which pay careful attention to the protection of data subjects. At the same time, the document highlights that a wide range of practitioners utilize data science techniques to analyze a breadth of human activities, which means that “the analytical tools of data science are being applied to a wide range of disciplines and sectors and there may be few commonalities across these, which poses a challenge in the development of a universal code of data ethics”.<sup>266</sup>

Guidance can also be found in 2017 *Guidelines on data protection in the context of Big Data*, from the Committee of Council of Europe Convention 108.<sup>267</sup> Among the recommendations are that any Big Data processing of personal data should comply with the requirement of free, specific, informed and unambiguous consent and the principles of purpose limitation, fairness and transparency. Additionally, data processors should provide easy ways for individuals to withdraw their consent and data processes and controllers should carry out risk assessments and assess the likely human rights impact of Big Data processing, for example, by establishing ethics committees. 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 publicly 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

#### **Definition. Open Data**<sup>268</sup>

Open Data is data that has been collected by an organization or institution and is subsequently made publicly available, subject to the necessary data protections.

<sup>264</sup> See European Parliament (2017) *Resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*. 2016/2225(INI).

<sup>265</sup> Recommendations include (but are not limited to): challenging assumptions on which existing ethical and legal regulations are based, in light of the emergence of new complexities posed by data analytics; facilitating new approaches to ethics review inside academia and industry; calibrating ethical assessment methods to Big Data practices; integrating ethics education into data science curricula; creating multidisciplinary networks of ethics engagement; setting standards for responsible cross-sector data sharing; and carrying out further research into the ethical implications of Big Data to identify opportunities to mitigate risks. Metcalf, J., E. Keller and D. Boyd (2016) ‘Perspectives on Big Data, Ethics, and Society’, *Council for Big Data, Ethics, and Society*, May 23.

<sup>266</sup> Accenture (2016) *Universal principles of data ethics: 12 guidelines for developing ethics codes*. Beaverton, United States: Accenture.

<sup>267</sup> CoE (2017) *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. Strasbourg, France: Council of Europe.

<sup>268</sup> Definitions of Open Data vary across jurisdictions and legal instruments as well as according to the purpose for which the term is being used. The general definition provided here draws from Open Knowledge International (2017) ‘What is Open Data?’, *Open Data Handbook*.

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.<sup>269</sup> Open Data encompasses open-source data, which refers to information that is publicly available (for example published on websites, in newspapers, in Craigslist and so on).<sup>270</sup> Simply put, all Open Data is publicly available. But not all publicly available data is Open Data.<sup>271</sup> Some Big Data may also be (or may become) Open Data; other Big Data remains in the control of the entity that collates it.

Calls for Open Data generally center around promoting transparency as an important tool in improving institutional responses and better decision-making by policymakers, practitioners and others. There is an increasing movement toward Open Data across many fields, including among anti-trafficking actors. One representative from a UN agency spoke about the usefulness of Open Data:

I would like to get to a point whereby our datasets are accessible on our website, with the necessary ethical and security protocols in place including to ensure anonymity of respondents. And you can access this data and there will be a write-up of how the data was collected and the methodologies behind it so that those who utilize this dataset are in a position to understand what they can and cannot do with the dataset.

There is also a movement toward government Open Data, which can serve anti-trafficking work. For example, in the United States, the 2013 *Open Data Memorandum* states: “in consultation with the best practices found in Project Open Data and to the extent permitted by law, agencies should prioritize the use of open formats that are non-proprietary, publicly available, and that place no restrictions upon their use”.<sup>272</sup> The United States government makes some datasets open and available *via* a search function, including datasets on human trafficking, with varying levels of restriction at Data.Gov.<sup>273</sup>

In considering the use of Open Data, it is important to explore both the opportunities of Open Data as well as the risks and issues associated with Open Data. These are discussed in turn below.

#### Issues with Open Data

- Opportunities of Open Data
- Risks and issues with Open Data

### 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. One staff member involved in sharing data from its service provision as Open Data described the objective being to share data securely but in ways that allowed others to access the datasets and contribute to the evidence base on human trafficking:

<sup>269</sup> To share alike refers to those who access open data also making their data available/open. Open Knowledge International (2017) ‘What is Open Data?’, *Open Data Handbook*.

<sup>270</sup> Open-Source Data is increasingly being analyzed by anti-trafficking actors and can be harnessed and analyzed by anti-trafficking actors to paint a clearer picture of trafficking situations.

<sup>271</sup> Sheriff, M. (2010) ‘What “open data” means - and what it doesn’t’, *opensource.com*, December 10.

<sup>272</sup> Burwell, S.M. et al. (2013) *Open Data Policy - Managing Information as an Asset*. Memorandum for the Heads of Executive Departments and Agencies M-13-13. United States: Project Open Data, paragraph 1(a).

<sup>273</sup> With regard to how the dataset is classified, data.gov notes: “This field refers to the degree to which this dataset *could be made available* to the public, regardless of whether it is currently available to the public. For example, if a member of the public can walk into your agency and obtain a dataset, that entry is public even if there are no files online. A *restricted public* dataset is one only available under certain conditions or to certain audiences (such as researchers who sign a waiver). A *non-public* dataset is one that could never be made available to the public for privacy, security, or other reasons as determined by your agency”. Government of the United States (2017) *Data.Gov*. United States: U.S. Government.

The aim... is to provide a mechanism to release the data in secure way... people such as [researchers] can help to develop the evidence-base for counter-trafficking policies and programs... We're hoping that the release of this kind will have quite a big impact. We also aim to move beyond victim data, let's say, data pertaining exclusively to victims as well as looking at other data relevant to human trafficking such as data on perpetrators, data on particular sectors possibly or data on government responses to trafficking as well.

The opening up and sharing of some datasets can be a cost effective and efficient way to conduct TIP research and analysis. As one researcher noted, there are existing datasets that could be used again to offer key findings and results:

A lot of these surveys are done once, they're looked at once, the data is buried in someone's computer and it could be used again and again.

Open Data is also democratic in that it promotes access. One researcher stressed the value of Open Data in the anti-trafficking field, particularly for smaller organizations and institutions that may lack the resources to conduct data collection on their own:

I would also say that the organizations that do have large data, if they would be willing to share that data [...] if they would make that publicly available it would completely change the landscape of what it was possible for smaller organizations to do. And I know there are some issues with archiving and with sharing data, but I think that the more that researchers in the field can put the time into making that data sharable and open access to others and are willing to share things like survey data or interview transcripts or other things in an anonymous form with other researchers, the more progress we're going to have as a field. Because then it will make it possible for smaller organizations to also not always need to start from scratch. And at the moment it feels like most of us who are doing this kind of research, with every new study we are starting from scratch because there is so little baseline data... The big organizations who have done a lot, if they could help build up a public evidence base on these topics, that would really facilitate people being able to do more with less funding and less resource.

As one staff member involved in this Open Data initiative explained, the approach was intended to meet the demand for TIP data but in a legal, safe and responsible way:

... because this information is so hard to come by and there are so few sources of information, [we] have just been inundated with requests for access to that data. And because it is so complicated to get through the de-identification process, to get through the whole legal process about allowing a researcher access to the disaggregated data, we started talking about how could we set up a platform where that work would happen on the front end and then once it was up and running, the amount of time and capacity it would take to allow new researchers could be very, very minimal. And so, we've basically gone through this process of identifying a platform, which will allow people who sign up access to the datasets that we publish on that platform and starting out the primary dataset will be a combination of [our] data.

This points to the high order question of the potential for harm when Open Data is not made available and used. That is, what are the consequences if trafficking responders cannot access Open Data in their efforts to design appropriate interventions and responses?

### 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.<sup>274</sup>

Certainly, care is needed in terms of data protection, to protect the privacy of all data subjects and adhere to legal requirements in terms of the de-identification and anonymization of personal or identifying. As one data collection staff working on Open Data noted:

...what we're asking for [project partners] to contribute is already de-identified to quite a high level, to the point where, most lawyers would say, "This is no longer personal data". [...] What then happens is we combine [the data] and we put it through another step of de-identification to a mathematical standard which is basically just to make certain that individuals cannot be picked out. So, I feel that we're in very safe territory on that. [...] We are hoping that by moving forward and showing that there is a concrete way of doing this that we can bring other actors on board.

How Open Data is effectively, ethically and legally de-identified and otherwise protected is, as noted above, fairly new terrain in the TIP field. This 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. The necessary procedures are also informed by the nature of the original dataset itself. Some data is more difficult to protect in ways that make it suitable as Open Data and other forms of data sharing.

Even when technology allows for adequate de-identification, knowledge of a particular country or environment may render some data recognizable. For example, geographic information (like a town or region of origin) may allow those familiar with the context to recognize information and thus individuals. This is particularly likely in cases where there are not large numbers of trafficked persons or there are few stakeholders involved in the anti-trafficking response. As one data collection staff member explained of their experience in developing Open Data, the organization opted to start with a limited number of variables, recognizing that some are still potentially identifying:

#### Questions relating to consent and Open Data

- ② Did initial consent foresee the possible use as Open Data?
- ② Are efforts needed to retroactively gain consent for data use?
- ② Is it realistic to be able to gain retroactive consent?
- ② Is it ethical to use the data?
- ② Is it ethical to *not* use the data, if it can enhance anti-trafficking efforts?
- ② In what contexts, if any, can consent be waived?

That's been a very arduous process, but we're going to be launching with about twenty variables which we have in common and most of those have to do with victim demographics, types of trafficking and exploitation, industries involved, that sort of thing. Geographic information is kind of the most identifying, so that's been a little bit problematic, but it will at least give some basic geographic information about where it took place.

<sup>274</sup> Granickas, K. (2015) *Ethical and Responsible Use of Open Government Data*. European Public Sector Information Platform Topic Report No. 2015/02.

Some governments and NGOs lack the skills and resources to process data into Open Data in a way that provides sufficient protections. In some cases, this may be a function of inadequate resources or lack of experience and capacity on data collection, processing and protection. But it may also be a function of Open Data, especially in the field of human trafficking, being a relatively new area of work in which the full range of risks and concerns have yet to be identified and addressed. The introduction and widespread application of ICT including third-party technology providers to anti-trafficking data may also add additional risks, as discussed above.

There are also questions to be asked about consent, as current Open Data initiatives draw from datasets that have been collected over years and some were collected very many years ago. Questions arise as to whether initial data collection foresaw this possible use and gathered consent for the transition to Open Data. If not, have efforts been made (or are efforts needed) to retroactively gain this consent? And is it realistic that consent issues could have been foreseen in earlier anti-trafficking data collection projects? Is it realistic to be able to gain retroactive consent and, in some cases (for example, victims who have reintegrated and moved on with their lives), might this type of contact breach privacy? Is it ethical not to use available data that could enhance our ability to combat human trafficking? Can consent can be waived in this context where a higher good is served by this information being made available?

There are also consent issues related to those who use and access Open Data. For instance, in terms of government Open Data efforts, the obligation to acquire informed consent would fall to the government itself, as opposed to anyone reusing the data. However, there is nonetheless a role for Open Data re-users in terms of considering and taking consent into account, particularly if there are reasonable grounds to believe that the re-use purpose is fundamentally different from the purpose to which the individual expressed consent at an earlier stage. There is an obligation to raise questions regarding the source of Open Data, whenever there are grounds to believe that there may be any sort of harm done to a particular individual or a societal group if data in hand is re-used and publicized.<sup>275</sup> When this is the case, the ethical decision may be not to use the data.

#### Questions relating to safety, security and Open Data

- ② Can Open Data be misused in a way that is dangerous?
- ② Does Open Data allow traffickers to find victims and/or their families?
- ② Does Open Data allow traffickers to identify hotspots for recruitment?
- ② Does Open Data help traffickers to better run their operations?

#### Box #16. Parameters of Open Data

The Open Data Charter (2015) sets out six principles of Open Data: 1) that it be open by default; 2) timely and comprehensive; 3) accessible and useable; 4) comparable and interoperable; 5) for improved governance and citizen engagement and 6) for inclusive development and innovation.<sup>276</sup>

It must also be considered whether access to Open Data poses any risk to safety and security. Can traffickers or exploiters access Open Data in ways that are dangerous? Will Open Data allow traffickers to find trafficking victims and their families or to identify hotspots for recruitment? Will

Open Data allow perpetrators to better understand how to run their operations, for instance, by developing new data-informed business models for recruitment of victims? Further, a distinction between the advisability of Open Data for protection and prosecution purposes may also be relevant.

<sup>275</sup> Granickas, K. (2015) *Ethical and Responsible Use of Open Government Data*. European Public Sector Information Platform Topic Report No. 2015/02.

<sup>276</sup> Carolan, L. (2016) *Open data, transparency and accountability: Topic guide*. Birmingham, United Kingdom: GSDRC, University of Birmingham.

As with other fields of data collection, principles are emerging that could be used to guide the use of Open Data in anti-trafficking work, such as the Open Data Charter described in Box #16 above. Responsible and ethical use of Open Data is an emerging issue and there are no set rules as to how to balance the risks involved in using Open Data (including those raised by issues of consent, privacy and security) against the advantages of such data.<sup>277</sup> As discussed above, there are a myriad potential benefits in using Open Data in the anti-trafficking field. Reconciling risks in the use of Open Data will likely require considering these issues on a case-by-case basis, informed by the different types of data, as well as the economic, social and political contexts in which data is collected.



## 7.4 Private sector engagement in anti-trafficking

Increased emphasis on corporate social responsibility and the pursuit by NGOs and international organizations of alternative funding sources has led to an increased number of actors from the private sector engaged in anti-trafficking work. Private sector actors may have a fundamentally different culture of information gathering, use and ownership to traditional anti-trafficking actors. There may also be differences of approach within and between private sector actors. One respondent described a spectrum of attitudes from different businesses when asked about the willingness of private sector actors to share information about TIP:

It depends on the jurisdiction of the company, where their head-office is located, and also in terms of their level of maturity in addressing social issues and human rights. Because for the leaders and innovators, they know transparency is key to building trust and they're willing to share some information... But for a lot of the companies [in this region], even the big ones, they're less inclined to share information due to a combination of factors: "saving/losing face", brand or reputational risk, questions of liability and the level of their maturity in the business and human rights framework. If they're not required by law to be more transparent and share the information, they're not going to share it willingly.

The same respondent noted that the willingness of private sector partners/companies to engage in meaningful ways differed:

From a compliance perspective, domestic laws are considered first and foremost. This is because there are on-going challenges for the application of international human rights laws for companies and countries: the issue of jurisdiction, liability and understanding of the laws itself. While the UK and U.S. have adopted legislations such as the California Transparency in Supply Chain Act and the UK Modern Slavery Act, there are no such equivalent legislations for companies in this region yet.

Nonetheless, issues arise in all business environments including when partners enter into non-disclosure agreements; 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, thus, is 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

### Issues with private sector engagement in anti-trafficking

- Supply chain accountability
- Public-private partnerships
- Defamation and other risks of collecting private sector data

<sup>277</sup> Granickas, K. (2015) *Ethical and Responsible Use of Open Government Data*. European Public Sector Information Platform Topic Report No. 2015/02, p. 8.



exploitation and other labor rights violations; and the idea that structural and systemic flaws may remain. These issues are further elaborated in the discussion below.

#### 7.4.1 Supply chain accountability

Perhaps the most common form of private sector engagement relates to supply chain accountability. Recent attention to ridding supply chains of “modern slavery”, human trafficking, forced labor 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 develop depending on 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.

The movement toward supply chain auditing (data collection on supply chains) has largely been driven by fiscal and jurisdictional constraints, which have, in some sectors, resulted in the public sphere taking a step back from scrutinizing the private sector and increasingly trusting the private sector to have oversight over its own supply chains. As one study notes:

States are increasingly entrusting corporations to govern themselves, either by supplementing official methods or by substituting their own inspection and monitoring responsibilities. The International Labour Organisation (ILO) reports a steep downturn in labour inspections in both the global South and North. This trend towards corporate self-governance is illustrated by the increasing adoption of voluntary corporate codes of conduct by states and international bodies.<sup>278</sup>

Self-auditing is also, arguably, a byproduct of both the 2011 *United Nations Guiding Principles on Business and Human Rights* (UNGPs)<sup>279</sup> and an expansion of consumer advocacy. Known as the “Ruggie principles” (for the then UN Special Representative on Business and Human Rights, John Ruggie), the UNGPs aim to offer global standards and guidelines to states and companies, to mitigate adverse human rights impacts linked to business activity.

While there are differences between public and private sector supply chains, the movement toward supply chain accountability affects both sectors. There are different approaches to supply chain auditing. Businesses can choose whether to use independent third-party auditors or in-house auditors. Increasingly NGOs are offering their services to audit supply chains, often signing non-disclosure agreements to do so. Third-party auditors are generally perceived to be more neutral and therefore “legitimate”. However, even third-party auditors are not always impartial.<sup>280</sup> Competing and conflicting considerations may arise depending on the perspective and situation of the stakeholder involved (including for example, the audited supplier, the organization assessing the supply chain or the worker involved in the specific supply chain and audit process).

---

<sup>278</sup> LeBaron, G. and J. Lister (2016) *Ethical Audits and the Supply Chains of Global Corporations*. Sheffield: Sheffield Political Economy Research Institute, p. 6.

<sup>279</sup> UN Secretary-General Special Representative (2011) *Report on the issue of human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, UN document A/HRC/17/31.

<sup>280</sup> LeBaron, G. and J. Lister (2016) *Ethical Audits and the Supply Chains of Global Corporations*. Sheffield, United Kingdom: Sheffield Political Economy Research Institute, p. 5.

Table #8. Some questions and considerations related to TIP data collection and supply chain auditing

### **In relation to the audited supplier**

- ② Can the supplier be compelled to share data it has a proprietary interest in, with a third-party? On what basis/authority? On what grounds can they refuse?
- ② What are the consequences of refusing to share data (for instance, commercial, owing to loss of reputation by not sharing data, even where it is not legally obliged to)?
- ② Where disclosure amounts to defamation, what recourse, if any, does the supplier have? From whom?
- ② What obligations (ethical and legal) does the supplier have to share/disclose data when supply chain information indicates exploitation or abuse?
- ② What are the implications for a supplier of not disclosing data about abuses/violations in its supply chain?
- ② What obligations (ethical and legal) does the supplier have to disclose findings and report exploitation and abuse? To whom do they report?
- ② What are the consequences of the supplier does not?

### **In relation to the organization(s) assessing supply chains**

- ② Where exploitation or abuses are identified in supply chains, do confidentiality agreements oblige the organization *not* to disclose these findings? Or are they obliged to disclose them and if so to who?
- ② Should or must law enforcers be contacted in the event that workers are identified as being potential victims of a crime in the context of their work? What are the consequences of doing so (or not doing so)?
- ② Is consent required to make such a disclosure? If so, whose consent is required? For example, the exploited worker or the company exploiting workers?
- ② What obligations, if any, does an actor have to disclose or not to disclose the irregular status or working situation of persons in supply chains? What are the consequences of their failure to do so?
- ② Is the organization protected from legal consequences of making disclosures where confidentiality agreements prohibit them from doing so, but it feels compelled to, for instance, to protect the rights of a child or identify victims of trafficking?
- ② Is the organization protected from legal consequences of *not* making such disclosures, for instance, where it fails to report the irregular status of a person who is being sought by authorities?
- ② Is the organization indemnified for any potential claims arising on the basis of defamation or other grounds?
- ② What opportunities exist to prevent the supplier from manipulating data to mislead the public on its supply chain management?

### **In relation to the worker**

- ② Have workers consented to the data they have provided to their employers being shared for non-employment purposes? What are the ramifications if they have not?
- ② What rights do workers have to participate in data collection about their employers' supply chain? What rights do workers have *not* to participate?
- ② What risks arise from having workers directly provide or verify data that may implicate employers? For instance, will workers face retribution from employers for speaking against them?
- ② Where an identified abusive or exploitative situation relates to a person who does not wish to be removed from that situation, is that person's non-consent relevant?
- ② What recourse, if any, do workers have when they are removed from situations that are determined to be exploitative, and deprived of the income and other benefits as a result?

Beyond questions such as these, broader issues exist with attempts to gather data pertaining to potential human trafficking in supply-chains. Some are relatively straight-forward (such as whether trafficking-related data collection in this commercial setting is subject to the same level of ethical and legal scrutiny that other data collection endeavors are and, if not, whether it should be). Some issues are more complex (for instance surrounding possible implications of having supply-chain audits publicly funded). Generally, these audits are internal and generate confidential data meaning that in essence, a donor is funding or subsidizing the private sector, with public funds used to generate what may be proprietary data.<sup>281</sup>

Partnerships to “clean up” supply chains may result in the private sector data protection approach having to be reconciled with the approach taken by non-private sector partner(s). Of importance is whether the private sector may (or may not) import the data laws and regulations that apply to them.

There are also questions about confidentiality or non-disclosure agreements, which are commonly required by private sector partners as part of an audit. Such agreements require auditors (and, in increasing cases, NGOs) conducting the audit not to disclose sensitive information (including human rights abuses and human trafficking) that they may find in supply chains. As one NGO director stated, access to data about supply chains and private sector activities has such limiting parameters that it becomes challenging for NGOs that could also take on a role of advocacy:

I think people end up on the wrong side of the argument because they’ll say, “We’re going to work with corporates”. They go to corporates and say, “Okay, tell us what you know” and the corporate says, “Fine there’s confidentiality”. And then that’s that. The information then stays in a pool. And so I think you have organizations [...] which know tons of things, they’re technically an NGO, but the amount of information they can share is a small proportion of what they know simply because they’ve signed service agreements and confidentiality agreements with the clients that they’ve helped. Well that doesn’t lead to transparency. That leads in the opposite direction.... And because of the way that the (anti-trafficking) community has... been so intent on jumping to that and saying, “Oh, we’ll go audit supply chains, help people gather that information” but they’re doing it on a confidential basis. ...that’s the best thing ever if somebody signs up to a confidentiality agreement and then tells you information about all sorts of activity which you know is risky to your business and they can’t tell anybody. And [the NGOs] think that they’re helping, but they’re not. They’re preventing the person from being held accountable.

Questions also need to be asked about the ethical and legal obligations for auditors to disclose abuses and violations and share their data with authorities. Such issues are further complicated in cases where NGOs engaged in these audits are also involved in working with and assisting trafficking victims and the complicated and contradictory space that they therefore inhabit.

It is also worth considering what impact audits have in real terms. One NGO director went on to describe the implications and potential limitations of confidentiality agreements for organizations engaged in supply chain assessments or audits:

...by locking something into confidentiality you are creating further risk to that victim. And to that NGO. Because they’ve got nowhere to turn to. And if they decide

---

<sup>281</sup> Proprietary data is internally generated data or documents that contain technical or other types of information controlled by a firm to safeguard its competitive edge. Proprietary data may be protected under copyright, patent or trade secret laws. Business Dictionary (2017) ‘Proprietary Data’, *Business Dictionary*.

to turn to somebody because they feel something is happening, then they're at risk of breach of contract and obviously then damages... It's making constraints and it's making boundaries which may need to be breached to do the right thing, whether it's to pursue a criminal case or compensation, pursuing civil litigation for compensation for the victim. But you can't because you're under this confidentiality [agreement].

One global study of supply chain audits noted of the auditing process: "Information about abuses and noncompliance is rarely made available to governments or consumers and, as such, they are rarely resolved". It suggested that audits were ineffective at improving standards, arguing that the regime may actually reinforce endemic problems in supply chains.<sup>282</sup> If data is collected, but not used to improve standards or combat human trafficking, what are the ethical implications? Many actors may be reluctant to bring attention to human trafficking in their supply chains or may not know how to proceed if trafficking cases are identified. As one staff member working on private sector engagement explained:

...what we've really heard from a lot of people is, "Okay, so we're presented with the vulnerabilities or we uncover a case of trafficking in our supply chain, what do we do with that information? There's nothing out there that tells us what is the system. Do we go to law enforcement? Do we shut down that facility where it's happening? What do we do?" ...the information that they're really craving is guidance on what are their options. Who can they engage in terms of NGOs, law enforcement? What are their available options?

There may also be unanticipated negative consequences of efforts to use data to scrutinize supply chains. For instance, the fact that certification processes can raise profits if certification is achieved and reduce profits if it is not seems, at face value, a sound strategy to incentivize companies to rid their supply chains of human trafficking and exploitation. But there may be risks that increased attention on supply chain transparency may divert attention from corporate complicity in exploitation. Will the impact of such a focus be to detract attention from promoting a decent work agenda?<sup>283</sup> Does such a focus complement or detract from existing efforts of businesses to implement the *UN Guiding Principles on Business and Human Rights*?<sup>284</sup> Will certification processes support the private sector to reduce exploitation in supply chains or simply put them out of business?

Even at the outset for such approaches, the lack of consistency between what is considered to amount to "human trafficking" or "slavery" or "modern slavery" in supply chains may have unintended and unanticipated consequences of lowering or raising the bar on what is considered to be exploitative, that will be transferred into any data collection efforts used to detect it. This, in turn, may result in reduced protection for victims of serious forms of exploitation or, conversely, may also result in unfair competition that causes harm to businesses and their employees. Questions are also raised in relation to those third-party actors who drive this attention on supply chains, including what the ethics are of monetizing the methodologies used to gather data for use in certification processes, by imbuing those methods with proprietary value.

---

<sup>282</sup> LeBaron, G. and J. Lister (2016) *Ethical Audits and the Supply Chains of Global Corporations*. Sheffield, United Kingdom: Sheffield Political Economy Research Institute.

<sup>283</sup> Decent work is measured according to ten substantive elements (employment opportunities; adequate earnings and productive work; decent working time; combining work, family and personal life; work that should be abolished; stability and security of work; equal opportunity and treatment in employment; safe work environment; social security; and social dialogue, employers' and workers' representation). ILO (2013) *Decent Work Indicators: Guidelines for Producers and Users of Statistical and Legal Framework Indicators*. Geneva, Switzerland: International Labour Organization.

<sup>284</sup> UN Secretary-General Special Representative (2011) *Report on the issue of human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN document A/HRC/17/31.

## 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 might 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.

A host of issues relating to the ownership of data emerges in such a scenario. Who owns the data that is collected from program beneficiaries (for example, trafficking victims)? Is it the beneficiary or the actor who provides the services? Do the confidentiality agreements in place attach to private sector partners as well as to public sector partners? Can the data collected from a beneficiary be shared within this network of actors, where no informed consent to do so was provided? Does the role of the private sector in such cases compromise beneficiaries who may raise serious complaints about the private sector? Are there adequate systems in place governing sharing of information between actors to guard the well-being of beneficiaries? When the data is anonymous can it be identified by inference through data analytics? What protections are in place to ensure that clients have consented to risks? When should or must service providers report information to law enforcers or other authorities about violations and even crimes they may uncover? And importantly, are the answers to these questions transparent?

Such questions may be difficult to answer when data collection is a secondary task to the primary work of service provision. Data protection measures may be reactively put in place, rather than proactively and coherently designed as part of the data collection framework. Another concern is the extent to which data is ethically and legally protected. Beneficiaries may have an understanding that they have a “privileged relationship” with service providers, being one in which the information they share cannot be disclosed. This may not be the case in fact or in law, but the assumption may not be correct. In addition, other non-funding private sector actors may be involved in maintaining the technological infrastructure that the NGO needs for its work (for example case management database, hotline, website etc.) and capture data from it. In such cases, questions may arise as to whether or not that tech-provider is a partner in the project with corresponding responsibilities (and rights) or is merely a paid service provider with responsibilities determined by contractual terms of its service agreement.

### Questions about ownership of data in public-private partnerships

- ② Who owns data collected from beneficiaries?
- ② Do confidentiality agreements attach to private sector partners?
- ② What data sharing is allowable without prior consent?
- ② What legal or ethical issues arise in sharing data within this network of actors?
- ② Are there adequate systems in place governing sharing of information between actors?
- ② What data protections are in place?
- ② When are service providers required to report any information to law enforcement?

Beyond data ownership, there are important questions to be asked about data sharing between private sector actors and those working in the public sector (for example, NGOs, international organizations and governments). That is, to what extent and when are private sector actors required to share data with anti-trafficking stakeholders? What are the legal obligations to report to law enforcement when a crime (of human trafficking or other

associated violations) has been committed and a company has collected data about this crime? What are the requirements to report exploitation and violence within business environments? And what are the consequences, if any, of not reporting?

A useful example comes from data collected by banks or other financial institutions that reveals that a private or legal person is engaging in trafficking in persons or may be benefiting from the exploitation of trafficked people. The entities that have this information may have a legal or ethical obligation to provide that information to authorities, whether through banking or other laws that provide exceptions to protecting data, for instance, where disclosure is necessary to detect or prevent crime. As one researcher observed:

#### Questions relating to data sharing between the private and public sector

- ② When are private sector actors required to share data with anti-trafficking stakeholders?
- ② When do legal obligations arise to report crimes to law enforcement?
- ② What are reporting requirements and expectations?
- ② What are the consequences for a lack of reporting?

...some groups have started looking at using financial crimes, so tracking down the money, using money laundering or corruption laws to tackle human trafficking issues. For money laundering claims, for example, they would need some data to show, to understand how the money flows from the victims or family of the victims to the recruitment agency, to the factories or company that used the labor.

#### Box #17. Data sharing between the humanitarian field and the private sector

World Vision International (WVI) has increased its use of cash-based programming, which changes the type of data collected as these programs require more engagement with financial service providers who have regulated systems and processes in place. Because this has required WVI to collect personal identification information data from beneficiaries and share it with third-parties, the organization has had to increase its understanding of data collection and protection particularly in terms of what data actually needs to be shared and what does not, to ensure compliance with both global standards and national policies to safeguard privacy and security of data.<sup>285</sup>

Or as one legal expert elaborated:

On the banking side because it's criminal, if you know that's happening you've got to report it. You cannot rely on confidentiality agreements. [...] If you're going to a bank and telling them, 'Oh by the way you're transacting with a trafficker or you're transacting with a drug trafficker or a human trafficker... or organized crime'. They don't say, 'Oh what should we do?' They have an obligation to

report it to the financial intelligence units who are law enforcement entity ultimately, and investigate it. They can't just sit there blithely and say 'Oh well, now what?' and, 'We didn't know'. You are under an obligation to know and to have done due diligence.

<sup>285</sup> World Vision (2017) *Discussion Paper: Data Protection, Privacy and Security for Humanitarian & Development Programs*. Federal Way, United States: World Vision International. Cash-based programming uses vouchers to deliver food assistance (either for a fixed quantity of food or for a fixed monetary value) and/or direct cash transfers to provide individuals with monetary assistance. Cash-based programming utilizes a market-based approach, whereby beneficiaries are equipped with the purchasing power to access assistance, directly purchasing commodities from contracted traders or shops and managing their own budgets. Cash-based programming can be combined with in-kind assistance. Yunus, E. and M. Markham (2016) 'Cash-based programming to address hunger in conflict-affected South Sudan: A Case study', *Disaster Management 2020*. Uxbridge, United States: World Vision International.

Regulations and requirements may have an impact in the other direction, when trafficking-related data is shared with such institutions, thereby entering into the realm of data that can, or perhaps must, be shared with authorities. For instance, partnerships with financial service providers may require the collection of personal data, as illustrated in Box #17 above.

### 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 and defamation charges, among others. As one researcher on business and human rights explained:

...inevitably researching business, you come into contact with and can be seen as a threat by business organizations because of the ways that activists have homed in on them and their responsibility for these practices. And so I think there are always legal concerns around that, around just needing to be extremely careful about any link that is made between these types of practices and the names of companies, because it could be damaging for them, but also because we're not journalists and we don't have the same rights and freedoms in terms of making public certain things.

In the same vein, one NGO director working on private sector engagement stressed the importance of taking seriously concerns about defamation:

...we take defamation extremely seriously... The NGOs that work with us... most of them understand the risk and difficulties of data sharing and particularly defamation. And to reduce the risk of everybody, we are careful about that.

In some cases, there are real risks posed to researchers and data collectors by private sector actors. The examples in Box #18 below include a case where researchers conducting data collection in New Zealand were threatened, stalked and faced degrading claims in the media and a case where defamation charges were brought against a researcher contracted by an NGO after the publication of the NGO funded report that alleged human and labor rights violations at a private company's pineapple processing plants.<sup>286</sup> Cases like these highlight the risks that researchers and workers themselves may face and which, in some cases, may deter them from conducting data collection about trafficking and exploitation when concerned about similar actions from private companies.

#### Box #18. Risks to data collectors

Researchers investigating trafficking in the foreign charter vessel sector of New Zealand's fishing industry reported being threatened and intimidated by those involved in the research (the researchers, respondents and translators), through direct confrontation and surveillance. The researchers described how private investigators were hired to investigate them to obtain information about the research and identify the research participants. On one occasion the researchers described a confrontation at a restaurant where the researchers were dining with crew members and coincidentally ran into the crew's former employer: "As we left the restaurant, both former New Zealand employers as well as three of their associates were waiting for us. They subjected us to intimidation to the point we were fearful for the safety of the participants, the translators, and ourselves. We were stalked and photographed, and our vehicles were followed which forced us to take a series of evasive maneuvers over the next hour to lose them".<sup>287</sup>

<sup>286</sup> Vartiala, S. et al. (2013) *Cheap Has a High Price. Summary Report*. Finland: Finnwatch.

<sup>287</sup> Stringer, C. and G. Simmons (2014) 'Stepping Through the Looking Glass: Researching Slavery in New Zealand's Fishing Industry', *Journal of Management Inquiry*, 24(3).

Following the publication of the January 2013 Finnwatch report *Cheap Has a High Price*, The Natural Fruit Company Ltd brought four interrelated civil and criminal claims against the individual researcher who coordinated field research and conducted migrant worker interviews, although Finnwatch maintained that the responsibility for the report lies with the organization (Finnwatch). The researcher was given a three-year suspended prison sentence.<sup>288</sup>



## 7.5 Summary

As capacity to collect and process data expands and accelerates, new opportunities emerge to harness this capacity towards strengthening anti-trafficking policy and practice. 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, the use of ICT can pose unpredictable risks, raising questions about who owns the data and how and with whom it is shared. At the same time, increased reliance on private sector partners to provide ICT raises a raft of issues and results in anti-trafficking stakeholders relinquishing some level of control over data to third-party, private sector actors. Where interests in data ownership conflict, there may be implications for data subjects and others. The role played by private sector actors in data collection also raises questions about the extent to which those actors have responsibilities to use that data in countering trafficking.

Related challenges emerge with increased collection of Big Data. While trafficking-specific Big Data is not yet developed, there is increased attention being paid to the possibility 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. Although individuals and communities can be impacted by Big Data, the lack of direct involvement of human subjects may result in a misconception that only minimum risk is involved, meaning that Big Data undertakings are not subject to ethical scrutiny. And dated legislative frameworks may be inadequate to address the challenges posed by Big Data. Accordingly, significant work is underway to adapt frameworks of protection to this new and evolving context.

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

Increased emphasis on corporate social responsibility and the pursuit by NGOs and international organizations of alternative funding sources have led to an increased number of private sector actors engaged in anti-trafficking work. Private sector actors may have a fundamentally different culture of information gathering, use and ownership to traditional anti-trafficking actors. There may also be differences of approach within and between private sector actors. Issues arise in all business environments including when partners enter into

---

<sup>288</sup> Finnwatch (2016) 'Thailand's top court dismisses criminal defamation case against Finnwatch researcher Andy Hall', *Finnwatch*, November 3; Finnwatch (2016) 'Finnwatch and retail chain S Group to testify at Andy Hall's trial', *Finnwatch*, July 7. See also Head, J. (2016) 'Andy Hall, British labour rights activist, flees Thailand', *BBC News*, November 7.



non-disclosure agreements; 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, thus, is 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.

As anti-trafficking becomes an ever-more 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 responses. In a best-case scenario, this will lead to strengthened data about trafficking situations that can inform tangible prevention and protection efforts. But in a worst-case scenario, the collision of interests can result in reduced accountability for trafficking and exploitation or even civil and criminal charges being laid against data collectors.

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 impacts 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 human trafficking.

There are no clear and easy “one size fits all” answers to emerging and continually evolving challenges. Responses that may be appropriate in one situation may be inappropriate in others. Some responses may also become redundant as dynamics shift and evolve. Therefore, the issues laid out above are offered for consideration and discussion, particularly for those who may be responsible for mitigating risks in the context of TIP data collection. In working towards stronger protection of data and upholding 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

TIP data collection must be guided by legal and ethical considerations to ensure that in our efforts to contribute to the evidence base informing a response to TIP, the persons involved in TIP data collection – whether data subjects, data collectors or anti-trafficking stakeholders – are protected from harm. While this paper has shown that the risk of harm is great when data collection is not conducted ethically and legally, what constitutes legal and ethical data collection remains a contested space with myriad tensions.

This paper is intended as a starting point in what we hope will be an inclusive, dynamic and reflective discussion of legal and ethical considerations in TIP data collection, towards determining how these considerations can be practically addressed. Our aim is to contribute to thinking and discussion on the 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 and administrative data). 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, 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.

Data ethics, data sciences and anti-trafficking are complex and relatively new and evolving fields. Their convergence raises a multitude of challenges that are yet to be resolved and will continue to be the subject of intense debate going forward. Definitive answers cannot be arrived at in the complex mix of law and ethics hailing from different perspectives and jurisdictions in an increasingly globalized world. However, this should not discourage efforts to do better. Rather, the challenges that emerge should inspire creative solutions and collaborations, to ensure that trafficking-related data collection evolves without losing sight of the core principles governing good practice.

Of benefit in resolving conflict is the fact that a useful overlap between what is ethical and what is legal can be found in the underlying principles that inform the frameworks for both. Indeed, ethical frameworks are anchored in principles that may be mirrored in the provisions set out in relevant laws or annexes thereto. While phrased differently across instruments and grouped in different ways, the fact that there is significant commonality between these principles across regions and countries, points to their value in offering a strong foundation for complying with both ethical and legal requirements. As evidenced below, principles relevant to TIP data collection are both ends in themselves and mutually supporting means of adhering to each other.

The following principles for data collection are based on those that frequently occur in both ethical guidance documents and legal frameworks. Both legal and ethical frameworks for data protection are anchored in such principles. Principles that are similar to those set out below can be found in national and regional data protection and privacy legislation and ethical frameworks across geographical regions, in international human rights law and in

internal guidelines of international organizations that collect data and self-regulate its protection. 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 the response 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 in data collection activities and that that participation is voluntary; data subjects should be engaged as partners in the design and implementation of the research or data collection study, 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 of 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.

## 9. Bibliography

Accenture (2016) *Universal principles of data ethics: 12 guidelines for developing ethics codes*. Beaverton, United States: Accenture. Available at:

[https://www.accenture.com/t20160629T012639Z\\_w\\_us-en\\_acnmedia/PDF-24/Accenture-Universal-Principles-Data-Ethics.pdf](https://www.accenture.com/t20160629T012639Z_w_us-en_acnmedia/PDF-24/Accenture-Universal-Principles-Data-Ethics.pdf)

ACFID (2016) *Principles and Guidelines for ethical research and evaluation in development*. Australia: Australia Council for International Development. Available at:

[https://acfid.asn.au/sites/site.acfid/files/resource\\_document/Principles-for-Ethical-Research-and-Evaluation-in-Development2016.pdf](https://acfid.asn.au/sites/site.acfid/files/resource_document/Principles-for-Ethical-Research-and-Evaluation-in-Development2016.pdf)

Achieng, R. (2016) 'Data Protection in the East African Community' in UNCTAD *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development. Available at: [https://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)

ADLS (2017) 'Administrative data introduction', *Guidance to apply for and use administrative data*. United Kingdom: Administrative Data Liaison Service. Available at: <http://www.adls.ac.uk/adls-resources/guidance/introduction/>

AEA (2004) *American Evaluation Association Guiding Principles for Evaluators*. United States: American Evaluation Association. Available at:

<https://www.eval.org/p/cm/ld/fid=51>

AES (2010) *Guidelines for the Ethical Conduct of Evaluations*. Lyneham, United Kingdom: Australasian Evaluation Society, Inc. Available at:

[https://www.aes.asn.au/images/stories/files/membership/AES\\_Guidelines\\_web\\_v2.pdf](https://www.aes.asn.au/images/stories/files/membership/AES_Guidelines_web_v2.pdf)

AFP (2018) 'Thailand to scan eyes of workers in notorious seafood industry', *Geo Television*, February 15. Available at <https://www.geo.tv/latest/182121-thailand-to-scan-eyes-of-workers-in-notorious-seafood-industry>

AfreA (2002) *The African Evaluation Guidelines*. Accra, Ghana: African Evaluation Association. Available at: <https://afrea.org/the-african-evaluation-guidelines/>

African Union (2014) *African Union Convention on Cyber Security and Personal Data Protection*. African Union. Available at: [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

*Allan v. the United Kingdom* (2002) European Court of Human Rights, 5 November 2002, No. 48539/99.

Andrews, D.C. and J.M. Newman (2012) 'Personal Jurisdiction and Choice of Law in the Cloud', *Maryland Law Review*, 73(1). Available at:

<https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3605&context=mlr>

Annas, G.J. and M.A. Grodin (1992) *The Nazi Doctors and the Nuremberg Code: Human Rights in Human Experimentation*. Oxford, United Kingdom: Oxford University Press.

APEC (2011) *Cross-Border Privacy Rules*. Singapore: Asia-Pacific Economic Cooperation Secretariat. Available at: <http://cbprs.org/>

APEC (2005) *Privacy Framework*. Singapore: Asia-Pacific Economic Cooperation Secretariat. Available at: [http://publications.apec.org/publication-detail.php?pub\\_id=390](http://publications.apec.org/publication-detail.php?pub_id=390)

ASEAN (2016) *Framework on Personal Data Protection*. Jakarta, Indonesia: Association of Southeast Asian Nations. Available at: <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>

ASEAN (2015) *Convention Against Trafficking in Persons, Especially Women and Children*. Jakarta, Indonesia: Association of Southeast Asian Nations. Available at: <https://asean.org/asean-convention-against-trafficking-in-persons-especially-women-and-children/>

ASEAN (2015) *Plan of Action Against Trafficking in Persons, Especially Women and Children*. Jakarta, Indonesia: Association of Southeast Asian Nations. Available at: <https://asean.org/asean-convention-against-trafficking-in-persons-especially-women-and-children/>

*B.B. v. France* (2009) European Court of Human Rights, 17 December 2009, No. 5335/06.

BakerHostetler (2015) *International Compendium of Data Privacy Laws*. United States: BakerHostetler. Available at: <https://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf>

Bali Process (2015) *Privacy and data protection laws of Bali process member states*. Bali, Indonesia: Bali Process. Available at: <https://www.baliprocess.net/UserFiles/baliprocess/File/Privacy%20and%20data%20protection%20laws%20of%20Bali%20Process%20members%20States.pdf>

Bankert, E.A. and R.J. Amdur (Eds.) (2006) *Institutional Review Board Management and Function*. Burlington, United States: Jones and Bartlett.

Berman, G. and K. Albright (2017) *Children and the Data Cycle: Rights and Ethics in a Big Data World*. UNICEF Office of Research Paper No. 2017-05. Florence, Italy: United Nations Children's Fund. Available at: [https://www.unicef-irc.org/publications/pdf/IWP\\_2017\\_05.pdf](https://www.unicef-irc.org/publications/pdf/IWP_2017_05.pdf)

Berman, G., J. Hart, D. O'Mathúna, E. Mattellone, A. Potts, C. O'Kane, J. Shusterman and T. Tanner (2016) *What We Know about Ethical Research Involving Children in Humanitarian Settings: An overview of principles, the literature and case studies*. Florence, Italy: United Nations Children's Fund. Available at: [https://www.unicef-irc.org/publications/pdf/IWP\\_2016\\_18.pdf](https://www.unicef-irc.org/publications/pdf/IWP_2016_18.pdf)

Bickert, M. and B. Fishman (2017) 'Hard Questions: How We Counter Terrorism', *Facebook Newsroom*, June 15. Available at: <https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/>

Bilger, V. and I. van Liempt (2009) 'Introduction' and 'Methodological and ethical dilemmas in research among smuggled migrants' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press.

Bloomberg (2017) 'Bloomberg, BrightHive, And Data for Democracy Launch Initiative to Develop Data Science Code of Ethics', *Bloomberg*, September 25. Available at: <https://www.prnewswire.com/news-releases/bloomberg-brighthive-and-data-for-democracy-launch-initiative-to-develop-data-science-code-of-ethics-300524958.html>

Boyd, Z. and K. Bales (2016) 'Getting What We Want: Experience and Impact in Research with Survivors of Slavery' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 173-190.

British Society of Criminology (2006) *Code of Ethics for Researchers in the Field of Criminology*. United Kingdom: British Society of Criminology. Available at: <http://www.britsocrim.org/docs/CodeofEthics.pdf>

Broad, E., A. Smith and P. Wells (2017) *Helping organisations navigate ethical concerns in their data practices*. Open Data Institute. Available at: <https://theodi.org/article/to-improve-open-data-help-publishers/>

Browne, M. (2017) 'YouTube Removes Videos Showing Atrocities in Syria', *New York Times* August 22. Available at: <https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html>

Brunovskis, A. (2012) 'A penny for your thoughts – paying participants in research' ['å betale deltakere I forskning'] in Fosshem, H. and H. Ingierd (Eds.) *Research and Money [Forskning og penger]*. Norway: Forskningsetiske komiteer.

Brunovskis, A. and R. Surtees (2010) 'Untold Stories: Biases and Selection Effects in Research with Victims of Trafficking for Sexual Exploitation', *International Migration*, 48(4), pp. 1-37.

Brunovskis, A. (2010) 'Irregular Migration in Norway' in Thomse, T.L. (Ed.) *Irregular Migration in a Scandinavian Perspective*. Netherlands: Shaker Publishing, pp. 48-49.

Brunovskis, A. and R. Surtees (2007) *Leaving the past behind? When victims of trafficking decline assistance*. Oslo: Fafo and Washington, D.C., United States: NEXUS Institute. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/03/leaving-the-past-behind-2007.pdf>

Buchinger, K. (2009) 'Protection Mechanisms and Ethics', *Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators*. Vienna, Austria: International Organization for Migration and Federal Ministry of the Interior of Austria. Available at: [http://publications.iom.int/system/files/pdf/guidelines\\_collection\\_data\\_iomvienna.pdf](http://publications.iom.int/system/files/pdf/guidelines_collection_data_iomvienna.pdf)

Burdick, A. (2017) 'The A.I. "Gaydar" study and the real dangers of Big Data', *New Yorker*, September 15. Available at: <https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data>

Burwell, S.M., S. VanRoekel, T. Park and D.J. Mancini (2013) *Open Data Policy - Managing Information as an Asset*. Memorandum for the Heads of Executive Departments and Agencies M-13-13. United States: Project Open Data. Available at: <https://project-open-data.cio.gov/policy-memo/>

Business Dictionary (2017) 'Proprietary Data', *Business Dictionary*. Available at: <http://www.businessdictionary.com/definition/proprietary-data.html>

Capri, A. (2018) 'How Blockchain Could Help End Modern Day Slavery in Asia's Exploitative Seafood Industry', *Forbes*, February 18. Available at: <https://www.forbes.com/sites/alexcapri/2018/02/14/how-blockchain-could-help-end-modern-day-slavery-in-asias-exploitative-seafood-industry/#23dfa3874b65>

Carolan, L. (2016) *Open data, transparency and accountability: Topic guide*. Birmingham, United Kingdom: GSDRC, University of Birmingham. Available at: <https://assets.publishing.service.gov.uk/media/5857fdb40f0b60e4a000d6/OpenDataTAGSDRC.pdf>

César, J., J. Debussche and B. Van Asbroeck (2017) 'White Paper - Data ownership in the context of the European data economy: Proposal for a new right', *Bird & Bird*. Available at: <https://www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy>

Chow, K.W. and N. Redfearn (2016) 'Data protection in ASEAN', *Rouse*. Available at: <http://www.rouse.com/magazine/news/data-protection-in-asean/>

CIOMS (2016) *International Ethical Guidelines for Health-related Research involving Humans*. Geneva, Switzerland: Council for International Organizations of Medical Sciences. Available at: <https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf>

Cockayne, J. and S. Walker (2016) *Fighting human trafficking in conflict: 10 ideas for Action by the United Nations Security Council*. United States: United Nations University. Available at: <https://unu.edu/fighting-human-trafficking-in-conflict>

CoE (2017) *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. Strasbourg, France: Council of Europe. Available at: <https://rm.coe.int/16806ebe7a>

CoE (2017) 'Modernization of the Data Protection Convention 108', *Council of Europe*, January 28. Available at: <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true>

CoE (2005) *Convention on Action against Trafficking in Human Beings*, ETS No. 197. Strasbourg, France: Council of Europe. Available at: <https://rm.coe.int/168008371d>

CoE (2005) *Convention on Action against Trafficking in Human Beings: Explanatory Report*. Strasbourg, France: Council of Europe. Available at: <https://rm.coe.int/16800d3812>

CoE (1987), *Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector*. Strasbourg: Council of Europe Committee of Ministers. Available at: <https://polis.osce.org/node/4656>

CoE (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108. Strasbourg, France: Council of Europe. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

CoE (1981) *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Explanatory Report*. Strasbourg, France: Council of Europe. Available at: <https://rm.coe.int/16800ca434>

CoE (1950) *European Convention on Human Rights*. Strasbourg, France: Council of Europe. Available at: [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf)

Commonwealth (2016) *Data Protection in the Commonwealth - Key Instruments and Current Practice*. London, United Kingdom: Commonwealth Secretariat. Available at: [https://unctad.org/meetings/en/Presentation/dtl\\_eweek2016\\_EBakibinga-Gaswaga\\_en.pdf](https://unctad.org/meetings/en/Presentation/dtl_eweek2016_EBakibinga-Gaswaga_en.pdf)



Coy, M. (2006) 'This morning I'm a researcher, this afternoon I'm an outreach worker: Ethical dilemmas in practitioner research international journal of social research methodology', *Theory and Practice*, 9(5), pp. 419–432.

Crosas, M., G. King, J. Honaker and L. Sweeney (2015) 'Automating Open Science for Big Data', *ANNALS of the American Academy of Political and Social Science*, 659(1). Available at: <https://gking.harvard.edu/files/gking/files/paper.pdf>

CTDC (2017) *Counter-Trafficking Data Collaborative*. Available at: <https://www.ctdatacollaborative.org/>

Cwikel, J. and E. Hoban (2005) 'Contentious issues in research on trafficked women working in the sex industry: Study design, ethics and methodology', *The Journal of Sex Research*, 42(4), pp. 306–316.

Dahinden, J. and D. Efonayi-Mader (2009) 'Challenges and strategies in empirical fieldwork with asylum seekers and migrant sex workers' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press.

datACT (2015) *Data Protection Standards for NGO Service Providers*. Germany: KOK and La Strada. Available at: [https://www.kok-gegen-menschenhandel.de/fileadmin/user\\_upload/medien/Projekte/dataact\\_standards\\_en\\_2018.pdf](https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/medien/Projekte/dataact_standards_en_2018.pdf)

Data Center Knowledge (2010) 'The Facebook Data Center FAQ', *Data Center Knowledge*. Available at: <http://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq>

De Wildt, R. (2016) 'Ethnographic Research on the Sex Industry: The Ambivalence of Ethical Guidelines' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 51-70.

Deloitte (2017) *Privacy is Paramount: Personal Data Protection in Africa*. Johannesburg, South Africa: Deloitte Touche Tohmatsu Limited. Available at: [https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za\\_Privacy\\_is\\_Paramount-Personal\\_Data\\_Protection\\_in\\_Africa.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf)

Dettmeijer-Vermeulen, C. (2013) *National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children in the Netherlands*. Berlin, Germany: Data Protection and the Right to Privacy for Marginalised Groups - A New Challenge in Anti-Trafficking Policies Conference. Available at: [http://www.dataact-project.org/fileadmin/user\\_upload/pdf/Corinne\\_Dettmeijer-Vermeulen.pdf](http://www.dataact-project.org/fileadmin/user_upload/pdf/Corinne_Dettmeijer-Vermeulen.pdf)

DFID (2011) *DFID Ethics Principles for Research and Evaluation*. United Kingdom: Department for International Development. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/67483/dfid-ethics-prcpls-rsrch-eval.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/67483/dfid-ethics-prcpls-rsrch-eval.pdf)

Di Francesco Maesa, C. (2016) 'Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)', *Eurojust.it*, May 24. Available at: <http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/>

DLA Piper (2017) *Data Protection Laws of the World Handbook*. London, United Kingdom: DLA Piper. Available at: <https://www.dlapiper.com/en/middleeast/insights/publications/2014/01/data-protection-laws-of-the-world-handbook/>

Ds Isaias Barreto Da Rosa (2016) 'ECOWAS Supplementary Act A/SA.1/01/10' in UNCTAD *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development, pp. 89-90.

Duffy, N. (2017) 'Insurance giant accidentally leaked HIV status of thousands of patients', *Pink News*, August 25. Available at: <http://www.pinknews.co.uk/2017/08/25/insurance-giant-accidentally-leaked-hiv-status-of-thousands-of-patients/>

Duong, K.A. (2015) 'Doing Human Trafficking Research: Reflections on Ethical Challenges', *Journal of Research in Gender Studies*, 5(2), pp. 171-190.

Dutch National Rapporteur (2013) *Trafficking in Human Beings. Ninth report of the Dutch National Rapporteur*. The Hague, Netherlands: Dutch National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. Available at: [https://www.dutchrapporteur.nl/binaries/national-rapporteur-on-trafficking-in-human-beings-and-sexual-violence-against-children.ninth-report-of-the-dutch-national-rapporteur.2014\\_tcm24-35346.pdf](https://www.dutchrapporteur.nl/binaries/national-rapporteur-on-trafficking-in-human-beings-and-sexual-violence-against-children.ninth-report-of-the-dutch-national-rapporteur.2014_tcm24-35346.pdf)

EAC (2009) *Framework for Cyber Laws*. Arusha, Tanzania: East African Community. Available at: <https://www.eac.int/infrastructure/communications-sector/94-sector/infrastructure/communications>

Easton, H. and R. Matthews (2016) 'Getting the Balance Right: The Ethics of Researching Women Trafficked for Commercial Sexual Exploitation' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 11-32.

EC (2018) 'National Rapporteurs and/or Equivalent Mechanisms', *Together Against Trafficking in Human Beings*. Brussels, Belgium: European Commission. Available at: [https://ec.europa.eu/anti-trafficking/national-rapporteurs-and-or-equivalent-mechanisms\\_en](https://ec.europa.eu/anti-trafficking/national-rapporteurs-and-or-equivalent-mechanisms_en)

EC (2018) 'What is personal data?', *Data Protection*. Brussels, Belgium: European Commission. Available at: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en)

EC (2017) 'Ethics', *Participant Portal H2020 Online Manual*. Brussels, Belgium: European Commission. Available at: [http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics\\_en.htm](http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm)

EC (2016) *Guidance note - Research on refugees, asylum seekers & migrants*. Brussels, Belgium: European Commission, Directorate-General. Available at: [http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide\\_research-refugees-migrants\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-refugees-migrants_en.pdf)

EC (2012) 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses', *European Commission*

Press Release Database, January 25. Available at: [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm](http://europa.eu/rapid/press-release_IP-12-46_en.htm)

EC (2010) *Communication on a Comprehensive Strategy on Data Protection in the European Union*. Brussels, Belgium: European Commission. Available at: <http://www.statewatch.org/news/2010/oct/eu-com-draft-communication-data-protection.pdf>

EC (2005) *The European Charter and Code for Researchers*. Brussels, Belgium: European Commission EURAXESS. Available at: <https://euraxess.ec.europa.eu/jobs/charter>

ECOWAS (2010) *Supplementary Act on Personal Data Protection Within ECOWAS*, A/SA.1/01/10. Nigeria: Economic Community of West African States. Available at: <https://ccdcoe.org/ecowas.html>

ECPAT International (2019) *Ethical considerations in research on sexual exploitation involving children*. Bangkok, Thailand: ECPAT International. Available at: <https://www.ecpat.org/wp-content/uploads/2019/04/ECPAT-International-Issues-Paper-Ethical-Considerations-Sexual-Exploitation-Children.pdf>

EDPS (2012) *Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – ‘The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016’*. Brussels, Belgium: European Data Protection Supervisor. Available at: [https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/edps\\_on\\_the\\_new\\_eu\\_anti-human\\_trafficking\\_strategy\\_1.pdf](https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/edps_on_the_new_eu_anti-human_trafficking_strategy_1.pdf)

Ehrenfreund, N. (2007) *The Nuremberg Legacy*. London, United Kingdom: Palgrave.

EIGE (2016) *Administrative data collection on violence against women: Good practices*. Lithuania: European Institute for Gender Equality. Available at: <https://eige.europa.eu/rdc/eige-publications/administrative-data-collection-violence-against-women-good-practices>

Elkhatib, Y. (2015) ‘Explainer: where is “the cloud” ...and who owns it?’, *The Conversation*, December 8. Available at: <https://theconversation.com/explainer-where-is-the-cloud-and-who-owns-it-51714>

Ellingwood, J. (2016) ‘An Introduction to Big Data Concepts and Terminology’, *Digital Ocean*, September 28. Available at: <https://www.digitalocean.com/community/tutorials/an-introduction-to-big-data-concepts-and-terminology>

English, A. (2017) ‘Mandatory Reporting of Human Trafficking: Potential Benefits and Risks of Harm’, *AMA Journal of Ethics*, 19(1). Available at: <https://journalofethics.ama-assn.org/article/mandatory-reporting-human-trafficking-potential-benefits-and-risks-harm/2017-01>

EPIC (2017) *Electronic Privacy Information Centre*. Available at: <https://epic.org/privacy/intl/coeconvention/>

European Parliament (2017) *Resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*. 2016/2225 (INI). Brussels, Belgium: European Parliament. Available at:

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+Vo//EN>

EU (2016) *Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. Brussels, Belgium: European Union. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.119.01.0089.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG)

EU (2016) *Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Brussels, Belgium: European Union. Available at: <https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>

EU (2016) 'The EU-U.S. Privacy Shield', *Data Protection*, July 12. Brussels, Belgium: European Union. Available at: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=605819](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605819)

EU (2013) *Annex 2: Proposals for Amendments regarding exemption for personal or household activities*. Brussels, Belgium: European Union. Available at: [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227\\_statement\\_dp\\_annex2\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf)

EU (2012) *Treaty on the Functioning of the European Union*, 2012/C 326/01. Brussels, Belgium: European Union. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>

EU (2011) *Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims*. Brussels, Belgium: European Union. Available at: [https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201136eu\\_en](https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201136eu_en)

EU (2000) *EU Charter of Fundamental Rights*. Brussels, Belgium: European Union. Available at: [https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights\\_en](https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en)

EU (1995) *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels, Belgium: European Union. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>

Facebook (2017) *Data Policy*. Menlo Park, United States: Facebook. Available at: [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy)

Finnwatch (2016) 'Finnwatch and retail chain S Group to testify at Andy Hall's trial', *Finnwatch*, July 7. Available at: <https://www.finnwatch.org/en/news/391-finnwatch-and-retail-chain-s-group-to-testify-at-andy-hall%27s-trial>

Finnwatch (2016) 'Thailand's top court dismisses criminal defamation case against Finnwatch researcher Andy Hall', *Finnwatch*, November 3. Available at: <https://www.finnwatch.org/en/news/417--thailand%27s-top-court-dismisses-criminal-defamation-case-against-finnwatch-researcher-andy-hall>

FMM West Africa (2017) *Support Free Movement of Persons & Migration in West Africa*. Available at: <https://fmmwestafrica.org/>

Fox, C. (2016) 'NHS trust fined for 56 Dean Street HIV status leak', *BBC News*, May 9. Available at: <http://www.bbc.com/news/technology-36247186>

FRA (2014) *Handbook on European Data Protection Law*. Vienna, Austria: European Union Agency for Fundamental Rights. Available at: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>

GAATW (2015) *Briefing Paper: Seeking Feedback from Trafficked Persons on Assistance Services: Principles and Ethics*. Bangkok, Thailand: Global Alliance Against Traffic in Women. Available at: [http://www.gaatw.org/publications/GAATW\\_BriefingPaper\\_Principles\\_and\\_Ethics.10.2015.pdf](http://www.gaatw.org/publications/GAATW_BriefingPaper_Principles_and_Ethics.10.2015.pdf)

Gerry, F., J. Muraszkiwicz and N. Vavoula (2016) 'The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns', *Computer Law & Security Review*, 32, pp. 205-217. Available at: <https://www.sciencedirect.com/science/article/pii/S0267364915001806>

Gibbs, S. (2017) 'WhatsApp faces EU taskforce over sharing user data with Facebook', *The Guardian*, October 26. Available at: <https://www.theguardian.com/technology/2017/oct/26/whatsapp-facebook-eu-data-article-29-working-party-taskforce-sharing-user>

Global Emancipation Network (2017) 'Tech Strikes Against Modern-Day Slavery', *Global Emancipation Network*, September 25. Available at: <http://www.globalemancipation.ngo/gen-splunk-human-trafficking/>

Government of Qatar (2016) *Law No. 13 Concerning Personal Data Protection (the Data Protection Law)*. Qatar: Government of Qatar. Available at: <https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf>

Government of the United States (2017) *Data.Gov*. United States: U.S. Government. Available at: <https://www.data.gov/>

Government of the United States (2017) 'Federal Policy for the Protection of Human Subjects', *Federal Register* 87(12), pp. 7149-7274. Washington, D.C., United States: U.S. Government. Available at: <https://www.gpo.gov/fdsys/pkg/FR-2017-01-19/pdf/2017-01058.pdf>.

Government of the United States (2013) *Violence Against Women Reauthorization Act*, 42 USC §13925(b) as amended. Washington, D.C., United States: U.S. Government.

Government of the United States (2009) *Code of Federal Regulations*, Title 45, 'Protection of Human Subjects'. Washington, D.C., United States: U.S. Government.

Government of the United States (1996) *Health Insurance Portability and Accountability Act*, Pub.L. 104–191, 110 Stat. 1936. Washington, D.C., United States: U.S. Government.

Government of the United States (1974) *Privacy Act*, 5 U.S.C. § 552a. Washington, D.C., United States: U.S. Government.

Government of the United States (1970) *Fair Credit Reporting Act*, 15 U.S.C. § 1681. Washington, D.C., United States: U.S. Government.

Granickas, K. (2015) *Ethical and Responsible Use of Open Government Data*. European Public Sector Information Platform Topic Report No. 2015/02. Available at: [https://www.europeandataportal.eu/sites/default/files/2015\\_ethical\\_and\\_responsible\\_use\\_of\\_open\\_government\\_data.pdf](https://www.europeandataportal.eu/sites/default/files/2015_ethical_and_responsible_use_of_open_government_data.pdf)

Greenleaf, G. (2014) *Privacy in the Other Seven South Asian (SAARC) States*. Oxford, United Kingdom: Oxford University Press.

Griffith, E. (2016) 'What is Cloud Computing?', *PC Magazine*, May 3. Available at: <https://www.pcmag.com/article2/0,2817,2372163,00.asp>

Guillemin, M. and L. Gillam (2004) 'Ethics, reflexivity and "ethically important moments"', *Research in Qualitative Inquiry*, 10(2), pp. 261–280.

HDT (2017) *Human Trafficking Data*. Available at: <http://www.humantraffickingdata.org/about>

Head, J. (2016) 'Andy Hall, British labour rights activist, flees Thailand', *BBC News*, November 7. Available at: <http://www.bbc.com/news/world-asia-37896421>

HHS (2017) *International Compilation of Human Research Standards*. United States: Office for Human Research Protections, U.S. Department of Health and Human Services. Available at: <https://www.hhs.gov/ohrp/international/compilation-human-research-standards/index.html>

Hogan Lovells (2017) *Asia Pacific Data Protection and Cyber Security Guide 2017*. London, United Kingdom: Hogan Lovells. Available at: [https://f.datasrvr.com/fr1/017/36473/Hogan\\_Lovells\\_Asia\\_Pacific\\_Data\\_Protection\\_and\\_Cybersecurity\\_Guide\\_2017.PDF](https://f.datasrvr.com/fr1/017/36473/Hogan_Lovells_Asia_Pacific_Data_Protection_and_Cybersecurity_Guide_2017.PDF)

Horning, A. and A. Paladino (2016) 'Walking the Tightrope: Ethical Dilemmas of Doing Fieldwork with Youth in US Sex Markets' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 205-226.

HRC (1994) *General Comment 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc. ICCPR/C/21/Add. 6. Geneva, Switzerland: Human Rights Council. Available at: [http://ccprcentre.org/page/view/general\\_comments/27798](http://ccprcentre.org/page/view/general_comments/27798)

HSRRC (2017) *Guidelines for Media Projects Involving Human Subjects*. Los Angeles, United States: Occidental College, Human Subjects Research Review Committee. Available at: [https://www.oxy.edu/sites/default/files/assets/.../hsrrc\\_media\\_project\\_guidelines.doc](https://www.oxy.edu/sites/default/files/assets/.../hsrrc_media_project_guidelines.doc)

HTD (2017) *Human Trafficking Data*. United States: Texas Christian University and National Institute of Justice. Available at: <http://www.humantraffickingdata.org/>

Hutt, R. (2016) 'Beyond bitcoin: 4 surprising uses for blockchain', *World Economic Forum*, December 13. Available at: <https://www.weforum.org/agenda/2016/12/fighting-human-trafficking-tracing-blood-diamonds-and-other-surprising-uses-for-blockchain>

Hynes, P. (2017) 'Trust and mistrust in the lives of forcibly displaced women and children', *Families, Relationships and Societies*, 6(2).

ICMPD (2015) *Targeting Vulnerabilities: The Impact of the Syrian War and Refugee Situation on Trafficking in Persons - A Study on Syria, Turkey, Lebanon, Jordan and Iraq*. Vienna, Austria: International Centre for Migration Policy Development. Available at: [https://www.icmpd.org/fileadmin/ICMPD-Website/Anti-Trafficking/Targeting\\_Vulnerabilities\\_EN\\_SOFT\\_.pdf](https://www.icmpd.org/fileadmin/ICMPD-Website/Anti-Trafficking/Targeting_Vulnerabilities_EN_SOFT_.pdf)

ICMPD (2009) *Anti-Trafficking Data Collection and Information Management in the European Union – A Handbook: The situation in the Czech Republic, Poland, Portugal and the Slovak Republic*. Vienna, Austria: International Centre for Migration Policy Development. Available at: [https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/icmpd\\_data\\_collection\\_and\\_information\\_management\\_2009\\_en\\_1.pdf](https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/icmpd_data_collection_and_information_management_2009_en_1.pdf)

ICMPD (2007) *Handbook on Anti-Trafficking Data Collection in South-Eastern Europe: Developing Regional Criteria*. Vienna, Austria: International Centre for Migration Policy Development and NEXUS Institute. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/03/data-collection-handbook.pdf>

ICO (2017) *Big Data, artificial intelligence, machine learning and data protection*. United Kingdom: Information Commissioner's Office, UK. Available at: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

ICO (2017) *The Guide to Data Protection*. United Kingdom: Information Commissioner's Office, UK. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/>

ICRC (2016) *Rules on Personal Data Protection*. Geneva, Switzerland: International Committee of the Red Cross. Available at: <https://shop.icrc.org/icrc-rules-on-personal-data-protection.html?store=default>

IFCR (2017) 'What is vulnerability?', *Disaster and Crisis Management*. Geneva, Switzerland: International Federation of Red Cross and Red Crescent Societies. Available at: <http://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/what-is-vulnerability/>

IFCR (1995) *Code of Conduct*. Geneva, Switzerland: Council of Delegates of the Red Cross and Red Crescent. Available at: <https://media.ifrc.org/ifrc/who-we-are/the-movement/code-of-conduct/>

ILO (2013) *Decent Work Indicators: Guidelines for Producers and Users of Statistical and Legal Framework Indicators*. Geneva, Switzerland: International Labour Organization. Available at: [https://www.ilo.org/wcmsp5/groups/public/---dgreports/---integration/documents/publication/wcms\\_229374.pdf](https://www.ilo.org/wcmsp5/groups/public/---dgreports/---integration/documents/publication/wcms_229374.pdf)

ILO (2012) *Harder to see, harder to count: survey guidelines to estimate forced labour of adults and children*. Geneva, Switzerland: International Labour Organization. Available at: [http://ilo.org/wcmsp5/groups/public/---ed\\_norm/---declaration/documents/publication/wcms\\_182096.pdf](http://ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_182096.pdf)

IOM (2017) 'Migrant Application (MigApp)', *ITC News*, January 16. Available at: <https://weblog.iom.int/migrant-application-migapp>

IOM (2017) 'UN Migration Agency, Polaris to Launch Global Data Repository on Human Trafficking', *Press Releases*, September 6. Geneva, Switzerland: IOM Available at: <https://www.iom.int/news/un-migration-agency-polaris-launch-global-data-repository-human-trafficking>

IOM (2010) *Data Protection Manual*. Geneva, Switzerland: International Organization for Migration. Available at: [https://publications.iom.int/system/files/pdf/iomdataprotection\\_web.pdf](https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf)

IOM (2009) *Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators*. Vienna, Austria: International Organization for Migration and Federal Ministry of the Interior of Austria. Available at: [http://publications.iom.int/system/files/pdf/guidelines\\_collection\\_data\\_iomvienna.pdf](http://publications.iom.int/system/files/pdf/guidelines_collection_data_iomvienna.pdf)

ISI (2010) *Declaration on Professional Ethics*. Iceland: International Statistical Institute. Available at: <https://www.scb.se/contentassets/db09cdb81aae41dd8a153bb366b00a36/isi-declaration-on-professional-ethics.pdf>

Karunakara, U. (2014) 'Data Sharing in a Humanitarian Context: The Experience of Médecins Sans Frontières' in Moore, S.A. (Ed.) *Issues in Open Research Data*. London, United Kingdom: Ubiquity Press, pp. 59-76.

Kelley, A. (2015) 'US human trafficking report under fire as Cuba and Malaysia are upgraded', *The Guardian*, July 27. Available at: <https://www.theguardian.com/global-development/2015/jul/27/us-human-trafficking-in-persons-report-under-fire-cuba-malaysia-upgraded>

Kelley, J. and B. Simmons (2014) 'Politics by Number: Indicators as Social Pressure in International Relations', *American Journal of Political Science*, 59(1). Available at: [https://dash.harvard.edu/bitstream/handle/1/13578027/157696/kelley\\_and\\_simmons\\_ajp\\_s.pdf?sequence=1](https://dash.harvard.edu/bitstream/handle/1/13578027/157696/kelley_and_simmons_ajp_s.pdf?sequence=1)

Kelly, L. and M. Coy (2016) 'Ethics as Process, Ethics in Practice: Researching the Sex Industry and Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 33-50.

Kenton, W. (2017) 'Supply Chain', *Markets & Economy*, November 2017. Available at <https://www.investopedia.com/terms/s/supplychain.asp>

Kerrand, P.L. and R. Dash (2017) 'Ethical Considerations in Mandatory Disclosure of Data Acquired While Caring for Human Trafficking Survivors', *AMA Journal of Ethics*, 19(1).

Latonero, M. and Z. Gold (2015) *Data, Human Rights & Human Security*. United States: Data & Society Research Institute. Available at: <https://datasociety.net/output/data-human-rights-human-security/>

*Leander v. Sweden* (1987) European Court of Human Rights, 26 March 1987, No. 9248/81.

LeBaron, G. and J. Lister (2016) *Ethical Audits and the Supply Chains of Global Corporations*. Sheffield, United Kingdom: Sheffield Political Economy Research Institute. Available at: <http://speri.dept.shef.ac.uk/wp-content/uploads/2016/01/Global-Brief-1-Ethical-Audits-and-the-Supply-Chains-of-Global-Corporations.pdf>



Leetaru, K. (2017) 'A Case Study in Big Data and the Replication Crisis', *Forbes*, September 1. Available at <https://www.forbes.com/sites/kalevleetaru/2017/09/01/a-case-study-in-big-data-and-the-replication-crisis/#23062f0b5105>

Leetaru, K. (2017) 'AI "Gaydar" and How the Future of AI will be Exempt from Ethical Review', *Forbes*, September 16. Available at: <https://www.forbes.com/sites/kalevleetaru/2017/09/16/ai-gaydar-and-how-the-future-of-ai-will-be-exempt-from-ethical-review/#76acd1bf2c09>

Leetaru, K. (2017) 'Is It Too Late For Big Data Ethics?', *Forbes*, October 16. Available at: <https://www.forbes.com/sites/kalevleetaru/2017/10/16/is-it-too-late-for-big-data-ethics/#5a0333383a6d>

Leetaru, K. (2017) 'Should Open Access and Open Data Come With Open Ethics?', *Forbes*, July 20. Available at <https://www.forbes.com/sites/kalevleetaru/2017/07/20/should-open-access-and-open-data-come-with-open-ethics/#403249025426>

Leetaru, K. (2016) 'Are Research Ethics Obsolete in the Era of Big Data?', *Forbes*, June 17. Available at: <https://www.forbes.com/sites/kalevleetaru/2016/06/17/are-research-ethics-obsolete-in-the-era-of-big-data/#6cc7fc7c7aa3>

Lewis, H. (2016) 'Negotiating Anonymity, Informed Consent and 'Illegality': Researching Forced Labour Experiences Among Refugees and Asylum Seekers in the UK' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 99-116.

Liberty Asia (2016) *Guidance Note on Use of Victims' Images*. Hong Kong: Liberty Asia.

Liberty Asia (2015) *Data Protection Guidelines*. Hong Kong: Liberty Asia.

Marcus, A. and R. Curtis (2016) 'No Love for Children: Reciprocity, Science, and Engagement in the Study of Child Sex Trafficking' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 191-204.

Markham, A. and E. Buchanan (2012) *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, Version 2.0. Association of Internet Researchers. Available at: <https://aoir.org/reports/ethics2.pdf>

Markova, E. (2009) 'The "insider" position: ethical dilemmas and methodological concerns in researching undocumented migrants with the same ethnic background' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press.

*Maximillian Schrems v Data Protection Commissioner* (2015) Judgment in Case C-362/14.

McAdam, M. (2016) 'Not All Prosecutions are Created Equal: Less counting prosecutions, more making prosecutions count', *Anti-Trafficking Review*, 6. Available at: <http://www.antitraffickingreview.org/index.php/atrjournal/article/view/176/164>

McVeigh, K. and M. Mahmood (2017) 'Facebook removes posts made by people smugglers aiming to lure migrants', *The Guardian*, August 25. Available at: [https://www.theguardian.com/global-development/2017/aug/25/facebook-removes-posts-made-by-people-smugglers-aiming-to-lure-migrants?CMP=share\\_btn\\_tw](https://www.theguardian.com/global-development/2017/aug/25/facebook-removes-posts-made-by-people-smugglers-aiming-to-lure-migrants?CMP=share_btn_tw)

Melrose, M. (2002) 'Labour pains: Some considerations on the difficulties of researching juvenile prostitution', *International Journal of Social Research Methodology*, 4(4), pp. 333–351.

Mendel, T., A. Puddephatt, B. Wagner, D. Hawtin and N. Torres (2012) *Global Survey on Internet Privacy and Freedom of Expression*. France: UNESCO. Available at: <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-internet-privacy-and-freedom-of-expression/>

Metcalf, J. (2014) 'Ethics Codes: History, Context and Challenges', *Council for Big Data, Ethics, and Society*, November 9. Available at: <http://bdes.datasociety.net/council-output/ethics-codes-history-context-and-challenges/>

Metcalf, J., E. Keller and D. Boyd (2016) 'Perspectives on Big Data, Ethics, and Society', *Council for Big Data, Ethics, and Society*, May 23. Available at: <http://bdes.datasociety.net/council-output/perspectives-on-big-data-ethics-and-society/>

Metcalf, J. and K. Crawford (2016) 'Where are the human subjects in Big Data research? The emerging ethics divide', *Big Data & Society*. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2779647](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2779647)

Mitroff, S. (2016) 'What is a bot?', *CNET*, May 5. Available at: <https://www.cnet.com/how-to/what-is-a-bot/>

*M.K. v. France* (2013) European Court of Human Rights, 18 April 2013, No. 19522/09.

*M.M. v. the United Kingdom* (2012) European Court of Human Rights, 13 November 2012, No. 24029/07.

Moniruzzaman, M. (2016) 'At the Organ Bazaar of Bangladesh: In Search of Kidney Sellers' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 227-248.

Narayanan, A. and V. Shmatikov (2008) *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*. Oakland, United States: IEEE Symposium on Security & Privacy. Available at: [https://www.researchgate.net/publication/265973077\\_Robust\\_De-anonymization\\_of\\_Large\\_Datasets\\_How\\_to\\_Break\\_Anonymity\\_of\\_the\\_Netflix\\_Prize\\_Dataset](https://www.researchgate.net/publication/265973077_Robust_De-anonymization_of_Large_Datasets_How_to_Break_Anonymity_of_the_Netflix_Prize_Dataset)

*Niemietz v. Germany* (1992) European Court of Human Rights, 16 December 1992, Application No. 13710/88.

Nissenbaum, H. (2004) 'Privacy as Contextual Integrity', *Washington Law Review*, 79. Available at <https://crypto.stanford.edu/portia/papers/RevNissenbaumDTP31.pdf>

Nuffield Council on Bioethics (2005) *The ethics of research related to healthcare in developing countries: a follow-up discussion paper*. London, United Kingdom: Nuffield Council on Bioethics. Available at: [http://nuffieldbioethics.org/wp-content/uploads/2014/07/HRRDC\\_Follow-up\\_Discussion\\_Paper.pdf](http://nuffieldbioethics.org/wp-content/uploads/2014/07/HRRDC_Follow-up_Discussion_Paper.pdf)

Nuremburg Military Tribunals (1949) *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law, No. 10, Volume 2*. Washington, D.C., United States: U.S. Government Printing Office.

OAS (2018) 'Department of International Law', *Secretariat for Legal Affairs*. Washington, D.C., esUnited Stat: Organization of American States. Available at: [http://www.oas.org/en/sla/dil/international\\_law.asp](http://www.oas.org/en/sla/dil/international_law.asp)

OAS (2017) *OAS: Data Protection*. Washington, D.C., United States: Organization of American States, Department of International Law Available at: [http://www.oas.org/dil/data\\_protection.htm](http://www.oas.org/dil/data_protection.htm)

OAS (2014) 'OAS' Work on Data Protection', *Data Protection*. Washington, D.C., United States: Organization of American States, Department of International Law. Available at: [http://www.oas.org/dil/data\\_protection\\_oas\\_work.htm](http://www.oas.org/dil/data_protection_oas_work.htm)

OAS (2011) *Draft: Preliminary Principles and Recommendations on Data Protection (the Protection of Personal Data)*, Document presented pursuant to General Assembly Resolution AG/RES.2514. Washington, D.C., United States: Organization of American States. Available at: [http://www.oas.org/dil/cp-cajp-2921-10\\_rev1\\_corr1\\_eng.pdf](http://www.oas.org/dil/cp-cajp-2921-10_rev1_corr1_eng.pdf)

ODI (2017) *The Data Ethics Canvas*. Open Data Institute. Available at: <https://theodi.org/the-data-ethics-canvas>

OECD (1980) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, France: Organization for Economic Cooperation and Development. Available at: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>

OHCHR (2016) *A Human Rights-Based Approach to Data: Leaving No-one Behind in the 2030 Development Agenda: Guidance Note to Data Collection and Disaggregation*. Geneva, Switzerland: Office of the United Nations High Commissioner for Human Rights. Available at: <https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf>

OHCHR (2013) *Who will be accountable? Human Rights and the Post-2015 Development Agenda*. Geneva, Switzerland: Office of the United Nations High Commissioner for Human Rights. Available at: <https://www.ohchr.org/Documents/Publications/WhoWillBeAccountable.pdf>

OHCHR (2002) *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, UN Doc E/2002/68/Add.1[4]. Available at: <https://www.ohchr.org/Documents/Publications/Traffickingen.pdf>

Open Knowledge International (2017) 'What is Open Data?', *Open Data Handbook*. Available at <http://opendatahandbook.org/guide/en/what-is-open-data/>

OSCE (2011) *Trafficking in Human Beings: Identification of Potential and Presumed Victims. A Community Policing Approach*. Vienna, Austria: Organization for Security and Cooperation in Europe. Available at: <https://www.osce.org/secretariat/78849>

Österreichischer Rundfunk and Others (2007) European Court of Justice, 8 November 2007, C-456/00, §73.

Open Knowledge International (2017) 'What is Open Data?', *Open Data Handbook*. Available at: <http://opendatahandbook.org/guide/en/>

Pesce, F. and I. Orfano (2009) 'Guideline 15', *Guidelines for the Collection of Data on Trafficking in Human Beings, Including Comparable Indicators*. Vienna, Austria: International Organization for Migration and Federal Ministry of the Interior of Austria. Available at: [http://publications.iom.int/system/files/pdf/guidelines\\_collection\\_data\\_iomvienna.pdf](http://publications.iom.int/system/files/pdf/guidelines_collection_data_iomvienna.pdf)

Plan International (2013) *Research Policy and Code of Conduct*. Woking, United Kingdom: Plan International. Available at: <https://plan-international.org/publications/research-policy-and-standards>

Plan International (2009) *How to: Include Child Protection in All Monitoring, Evaluation and Research Initiatives*. Woking, United Kingdom: Plan Ltd. Unpublished document.

Plan International (2009) *How to: Include Ethical Standards in all Monitoring, Evaluation and Research Initiatives*. Woking, United Kingdom: Plan Ltd. Unpublished document.

Planet Biometrics (2015) 'Gulf countries move towards integrated biometric database', *Planet Biometrics*, February 9. Available at: <http://www.planetbiometrics.com/article-details/i/2681/>

*PLoS Medicine* Editors (2009) 'Ethics Without Borders', *PLOS Medicine*, 6(7). Available at: <https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000119>

Privacy International (2017) *Privacy International*. Available at: <https://www.privacyinternational.org/node/44>

RCUK (2013) *RCUK Policy and Guidelines on Governance of Good Research Conduct*. United Kingdom: Research Councils UK. Available at: <http://www.rcuk.ac.uk/documents/reviews/grc/rcukpolicyguidelinesgovernancegoodresearchconduct-pdf/>

Reason (2015) *Ethics for Research with Children, Young People and Vulnerable Adults*. United Kingdom: Reason. Available at: [http://www.reason-network.org.uk/wp-content/uploads/2012/07/ethics\\_for\\_research\\_with\\_children.pdf](http://www.reason-network.org.uk/wp-content/uploads/2012/07/ethics_for_research_with_children.pdf)

Rende-Taylor, L. and M. Sullivan (2012) 'Raising the Standard of Ethics and Human Rights Among Anti-human Trafficking Responders in the Mekong Region', *Human Rights Education in Asia-Pacific*, 3, pp. 55-69.

Responsible Data Forum (2016) *The Hand-Book of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment*. Responsible Data Forum. Available at: <https://responsibledata.io/resources/handbook/assets/pdf/responsible-data-handbook.pdf>

Responsible Data Forum (2014) *Primer on Responsible Data in Development*. Responsible Data Forum. Accessible at: <https://responsibledata.io/forums/primer-responsible-data-in-development/>

RIN (2010) *Quality assurance and assessment of scholarly research: A guide for researchers, academic administrators and librarians*. United Kingdom: Research Information Network. Available at: [http://www.rin.ac.uk/system/files/attachments/Quality\\_Assurance\\_screen\\_o.pdf](http://www.rin.ac.uk/system/files/attachments/Quality_Assurance_screen_o.pdf)

- Rivard, N. (2015) 'New 'TIP' Line App', *Airline Ambassadors International*, September 19. Available at: <http://airlineamb.org/2015/09/19/aais-new-tip-line-app/#.Wh3fL7Q-dol>
- Rodriguez, G. and A. Patel (2016) *Life after Salesforce*. Medford, United States: Tufts University.
- Roth, P., B.H. Uhl, M. Wijers and W. Zikkenheiner (2015) *Data Protection Challenges in Anti-Trafficking Policies: A Practical Guide*. Berlin, Germany: KOK e.V. Available at: [https://www.kok-gegen-menschenhandel.de/fileadmin/user\\_upload/medien/KOK\\_informiert/datAct\\_engl\\_Online.pdf](https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/medien/KOK_informiert/datAct_engl_Online.pdf)
- Rothman, E.F. et al. (2018) 'Ethical and Practical Considerations for Collecting Research-Related Data from Commercially Exploited Children', *Behavioral Medicine*, 44(3), pp. 250-258.
- S. and Marper v. the United Kingdom* (2008) European Court of Human Rights, 4 December 2008, Nos. 30562/04 and 30566/04.
- Schecke & Eifert* (2010) European Court of Justice, 9 November 2010, C-92/09 and C93/09.
- Schenk, K. and J. Williamson (2005) *Ethical Approaches to Gathering Information from Children and Adolescents in International Settings: Guidelines and Resources*. Washington, D.C., United States: Population Council. Available at: <https://www.popcouncil.org/uploads/pdfs/horizons/childrenethics.pdf>
- Scheper Hughes, N. (2016) 'On Adopting Heretical Methods: From Barefoot to Militant to Detective Anthropology' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 249-272.
- Schlanger, Z. (2017) 'The UN wants Facebook to fix its human trafficking problem', *Quartz*, September 28. Available at: <https://qz.com/1089835/facebook-and-whatsapp-gives-migrant-smugglers-a-platform-according-to-the-un/>
- Schopper, D., R. Upshur, F. Matthys, J.A. Singh, S.S. Bandewar, A. Ahmad and E. van Dongen (2009) 'Research ethics review in humanitarian contexts: The experience of the independent ethics review board of Medecins Sans Frontieres' *PLOS Medicine*, 6. Available at: <https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000115>
- Schriver, R.R. (2002) 'You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission', *Fordham Law Review*, 70(6). Available at: <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3848&context=flr>
- Scott, S. and A. Geddes (2016) 'Ethics, Methods and Moving Standards in Research on Migrant Workers and Forced Labour' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 117-136.
- Sheriff, M. (2010) 'What "open data" means - and what it doesn't', *opensource.com*, December 10. Available at: <https://opensource.com/government/10/12/what-%22open-data%22-means-%E2%80%93-and-what-it-doesn%E2%80%99t>
- Siegel, D. (2016) 'Ethnicity, Crime and Sex Work: A Triple Taboo' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 71-84.

- Siegel, D. and R. de Wildt (Eds.) (2016) *Ethical Concerns in Research on Human Trafficking*. New York, United States: Springer.
- Siegel, D. and R. de Wildt (2016) 'Introduction: The Variety of Ethical Dilemmas' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 1-7.
- Smith, B. (2018) 'A problem Congress should solve', *Microsoft On the Issues*, February 27. Available at: <https://blogs.microsoft.com/on-the-issues/2018/02/27/a-problem-congress-should-solve/>
- Spenser, T. (2012) 'GCC to fingerprint, iris scan migrant workers for health purposes', *Biometric Update*, October 9. Available at: <http://www.biometricupdate.com/201210/gcc-to-fingerprint-iris-scan-migrant-workers-for-health-purposes>
- Staring, R. (2009) 'Different methods to research irregular migration' in Van Liempt, I. and V. Bilger (Eds.) *The Ethics of Migration Research Methodology: Dealing with Vulnerable Immigrants*. East Sussex, United Kingdom: Sussex Academic Press.
- State of Hesse (1970) *Datenschutzgesetz* [Data Protection Act] of October 7, 1970, Hessisches Gesetz-und Verordnungsblatt I.
- Stringer, C. and G. Simmons (2014) 'Stepping Through the Looking Glass: Researching Slavery in New Zealand's Fishing Industry', *Journal of Management Inquiry*, 24(3).
- Surtees, R. (2014) 'Another side of the story: challenges in research with unidentified and unassisted trafficking victims' in Yea, S. (Ed.) (2017) *Human Trafficking in Asia: Forcing Issues*. New York: Routledge.
- Surtees, R. (2014) *Traffickers and Trafficking. Challenges in researching human traffickers and trafficking operations*. Geneva, Switzerland: International Organization for Migration and Washington, D.C.: NEXUS Institute. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/02/traffickersandtrafficking1.pdf>
- Surtees, R. (2013) *Ethical principles in the re/integration of trafficked persons. Experiences from the Balkans*. Washington, D.C., United States: NEXUS Institute and Brussels: King Baudouin Foundation. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/02/ethical-principles-for-the-reintegration-of-trafficked-persons.pdf>
- Surtees, R. (2010) *Monitoring anti-trafficking re/integration programmes. A manual*. Brussels, Belgium: King Baudouin Foundation & Washington D.C., United States: NEXUS. Available at: [https://nexushumantrafficking.files.wordpress.com/2015/03/monitoring-at-reintegration-programmes\\_manual\\_nexus.pdf](https://nexushumantrafficking.files.wordpress.com/2015/03/monitoring-at-reintegration-programmes_manual_nexus.pdf)
- Surtees, R. (2009) *Anti-Trafficking Data Collection and Information Management in the European Union - A Handbook: The situation in the Czech Republic, Poland, Portugal and the Slovak Republic*. Vienna, Austria: International Centre for Migration Policy Development. Available at: [https://nexushumantrafficking.files.wordpress.com/2015/03/handbook\\_english.pdf](https://nexushumantrafficking.files.wordpress.com/2015/03/handbook_english.pdf)
- Surtees, R. (2008) 'Traffickers and Trafficking in South and Eastern Europe: Considering the Other Side of Human Trafficking', *European Journal of Criminology*, 5(1).

Surtees, R. (2007) *Handbook on Anti-Trafficking Data Collection in South-Eastern Europe: Developing Regional Criteria*. Vienna, Austria: International Centre for Migration Policy Development. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/03/data-collection-handbook.pdf>

Surtees, R. (2007) *Listening to Victims: Experiences of Identification, Return Assistance in SE Europe*. Vienna, Austria: ICMPD & NEXUS Institute. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/03/listening-to-victims.pdf>

Surtees, R., A. Brunovskis and L.S. Johnson (2019) *The Science (and Art) of Understanding Trafficking in Persons. Identifying 'Good Practice' in TIP Data Collection*. Washington, D.C., United States: NEXUS Institute. Available at: <https://nexusinstitute.net/past-projects/global-data-collection/>

Surtees, R. and A. Brunovskis (2016) 'Doing No Harm - Ethical Challenges in Research with Trafficked Persons' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 137-154.

Surtees, R. and S. Craggs (2010) *Beneath the Surface. Methodological Issues in Research and Data Collection with Assisted Trafficking Victims*. Geneva, Switzerland: IOM and Washington, D.C.: NEXUS Institute. Available at: [https://nexushumantrafficking.files.wordpress.com/2015/03/beneath-the-surface\\_methodological-issues\\_nexus.pdf](https://nexushumantrafficking.files.wordpress.com/2015/03/beneath-the-surface_methodological-issues_nexus.pdf)

Sweeney, L. (2004) 'Navigating Computer Science Research Through Waves of Privacy Concerns: Discussions among Computer Scientists at Carnegie Mellon University', *ACM Computers and Society*, 34(1).

*Szabo v Hungary* (2016) European Court of Human Rights No. 37138/14.

Tech Terms (2017) 'ICT Definition', *Tech Terms*. Available at: <https://techterms.com/definition/ict>

Testa, A.C., I. Birdthistle, J. Amoura, S. Mayhew, O. Ross-Hurst and T. Boler (2011) *A Matter of Principle: A Family Planning NGO Experience Setting up an Independent Ethics Review Committee (Poster)*. United States: Advancing Ethical Research Conference.

Trunomi (2018) *EU General Data Protection Regulation Portal*. Available at: <https://www.eugdpr.org/>

The Commonwealth (2018) 'Member Countries', *The Commonwealth*. Available at: <http://thecommonwealth.org/member-countries>

The Freedom Story (2017) *Ethical Storytelling*. Available at: <http://ethicalstorytelling.com/about/>

Transparency International (2001) *A Statement of Vision, Values and Guiding Principles for Transparency International*. Berlin: Transparency International. Available at: [https://www.transparency.org/whoweare/accountability/a\\_statement\\_of\\_vision\\_values\\_and\\_guiding\\_principles\\_for\\_ti/3/](https://www.transparency.org/whoweare/accountability/a_statement_of_vision_values_and_guiding_principles_for_ti/3/)

Twitter (2017) 'Guidelines for Law Enforcement', *General Policies*. Available at: <https://support.twitter.com/articles/41949#>

Twitter (2017) 'Private information posted on Twitter', *General Policies*. Available at: <https://support.twitter.com/articles/20169991>

Tyldum, G. (2012) 'Ethics or access? Balancing informed consent against the application of institutional, economic or emotional pressures in recruiting respondents for research', *International Journal of Social Research Methodology*, 15(3).

UKRIO (2009) *Code of Practice for Research*. United Kingdom: UK Research Integrity Office. Available at: <http://ukrio.org/publications/code-of-practice-for-research/>

UKRIO (2009) '3.14 Peer Review', *Code of Practice for Research*. United Kingdom: UK Research Integrity Office. Available at: <http://ukrio.org/publications/code-of-practice-for-research/3-0-standards-for-organisations-and-researchers/3-14-peer-review/>

United Nations (2015) 'Professional Ethics', *United Nations Fundamental Principles of Official Statistics*. Geneva, Switzerland: United Nations.

United Nations (2015) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, UN Doc A/HRC/29/32.

United Nations (2000) *Convention Against Transnational Organized Crime*, UN Doc A/RES/55/25. Available at: <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>

United Nations (2000) *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*, UN Doc A/45/49. Available at: <https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx>

United Nations (1966) *International Covenant on Civil and Political Rights*, UN Doc A/RES/2200A(XXI). Available at: <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>

UNCTAD (2016) *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Geneva, Switzerland: United Nations Conference on Trade and Development. Available at: [https://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)

UN Global Pulse (2016) *Data Innovation Risk Assessment Tool*. United Nations Global Pulse. Available at: <http://www.unglobalpulse.org/privacy/tools>

UNHCR (2015) *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*. Geneva, Switzerland: United Nations High Commissioner for Refugees. Available at: <https://www.refworld.org/docid/55643c1d4.html>

UNIAP (2008) *Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming*. Bangkok, Thailand: United Nations Inter-Agency Project on Human Trafficking. Available at: [http://www.endvawnow.org/uploads/browser/files/Ethics\\_Guidelines\\_Trafficking\\_UNIAP\\_2008.pdf](http://www.endvawnow.org/uploads/browser/files/Ethics_Guidelines_Trafficking_UNIAP_2008.pdf)



UNICEF (2006) *Guidelines on the Protection of Child Victims of Trafficking*. New York, United States: United Nations Children's Fund. Available at: [https://www.unicef.org/protection/Unicef\\_Victims\\_Guidelines\\_en.pdf](https://www.unicef.org/protection/Unicef_Victims_Guidelines_en.pdf)

UNICEF (2003) *Principles and Guidelines for Ethical Reporting: Children and Young People under 18 years old*. New York, United States: United Nations Children's Fund. Available at: [https://www.unicef.org/uganda/Guidelines\\_for\\_Reporting\\_on\\_Children1.pdf](https://www.unicef.org/uganda/Guidelines_for_Reporting_on_Children1.pdf)

UNODC (2016) *Global Report on Trafficking in Persons*. Vienna, Austria: United Nations Office on Drugs and Crime. Available at: [https://www.unodc.org/documents/data-and-analysis/glotip/2016\\_Global\\_Report\\_on\\_Trafficking\\_in\\_Persons.pdf](https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf)

UNODC (2012) *Guidance Note on "abuse of a position of vulnerability" as a means of trafficking in persons in Article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*. Vienna, Austria: United Nations Office on Drugs and Crime. Available at: [https://www.unodc.org/documents/human-trafficking/2012/UNODC\\_2012\\_Guidance\\_Note\\_-\\_Abuse\\_of\\_a\\_Position\\_of\\_Vulnerability\\_E.pdf](https://www.unodc.org/documents/human-trafficking/2012/UNODC_2012_Guidance_Note_-_Abuse_of_a_Position_of_Vulnerability_E.pdf)

UN Secretary-General (2016) 'Annex: Special Report of the Office of the Special Representative of the Secretary-General on Sexual Violence in Conflict', *Letter to the President of the Security Council*, 21 December 2016, UN Doc S/2016/1090.

UN Secretary-General Special Representative (2011) *Report on the issue of human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN document A/HRC/17/31.

United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1978) *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Bethesda, United States: National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Available at: [https://videocast.nih.gov/pdf/ohrp\\_appendix\\_belmont\\_report\\_vol\\_2.pdf](https://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf)

University of Surrey Library (nd) 'Qualitative Research', *Introduction to Research*. United Kingdom: University of Surrey. Available at: [http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page\\_52.htm](http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page_52.htm)

University of Surrey Library (nd) 'Quantitative Research', *Introduction to Research*. United Kingdom: University of Surrey. Available at: [http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page\\_43.htm](http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page_43.htm)

University of Surrey Library (nd) 'Triangulation', *Introduction to Research*. United Kingdom: University of Surrey. Available at: [http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page\\_29.htm](http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page_29.htm)

Vartiala, S., H. Purje, A. Hall, K. Vihersalo and A. Aukeala (2013) *Cheap Has a High Price. Summary Report*. Finland: Finnwatch. Available at: [https://www.finnwatch.org/images/cheap%20has%20a%20high%20price\\_exec%20summary\\_final.pdf](https://www.finnwatch.org/images/cheap%20has%20a%20high%20price_exec%20summary_final.pdf)

- Verma, I. (2014) 'Editorial Expression of Concern and Correction', *Proceedings of the National Academy of Sciences*, 111(29).
- WANGO (2004) *Code of Ethics & Conduct for NGOs*. World Association of Non-Governmental Organizations. Available at: <http://ethics.iit.edu/ecodes/node/4976>
- Warden, T. (2013) 'Feet of clay: confronting emotional challenges in ethnographic experience', *Journal of Organizational Ethnography*, 2(2), pp. 150-172.
- Warnath, S. (2008) *Efforts to Combat Trafficking in Human Beings in the OSCE Area: Co-Ordination and Reporting Mechanisms*. Vienna, Austria: Organization for Security and Co-Operation in Europe. Available at: <https://nexushumantrafficking.files.wordpress.com/2015/03/osce-2008-annualreport.pdf>
- Whipple, K. (2017) 'Big Data is reducing human trafficking in India', *MAPR Data Technologies*, May 30. Available at: <https://mapr.com/blog/how-big-data-fights-human-trafficking/>
- WHO (2011) *Standards and Operational Guidance for Ethics Review of Health-Related Research with Human Participants*. Geneva, Switzerland: World Health Organization. Available at: <https://www.who.int/ethics/publications/9789241502948/en/>
- WHO (2003) *Ethical and Safety Recommendations for Interviewing Trafficked Women*. Geneva, Switzerland: World Health Organization. Available at: [https://www.who.int/mip/2003/other\\_documents/en/Ethical\\_Safety-GWH.pdf](https://www.who.int/mip/2003/other_documents/en/Ethical_Safety-GWH.pdf)
- WMA (1964) *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects*. Helsinki, Finland: World Medical Association. Available at: <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>
- World Vision (2017) Discussion Paper: Data Protection, Privacy and Security for Humanitarian & Development Programs. Federal Way, United States: World Vision International. Available at: <http://wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs>
- Yea, S. (2016) 'Trust, Rapport, and Ethics in Human Trafficking Research: Reflections on Research with Male Laborers from South Asian in Singapore' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. Switzerland: Springer International Publishing, pp. 155-172.
- Yunus, E. and M. Markham (2016) 'Cash-based programming to address hunger in conflict-affected South Sudan: A Case study', *Disaster Management 2020*. Uxbridge, United Kingdom: World Vision International. Available at: <https://www.wvi.org/disaster-management/publication/cash-based-programming-address-hunger-conflict-affected-south-sudan-case-study>
- Zang, J., K. Dummit, J. Graves, P. Lisker and L. Sweeney (2015) 'Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third-parties by Mobile Apps', *Technology Science*, October 30. Available at: <https://techscience.org/a/2015103001/>
- Zakharov v Russia* (2015) European Court of Human Rights No. 47143/06.

Zhang, S.X. (2016) 'The Ethical Minefield in Human Trafficking Research - Real and Imagined' in Siegel, D. and R. de Wildt (Eds.) *Ethical Concerns in Research on Human Trafficking*. New York, United States: Springer, pp. 85-98.

ZICO Law (2016) *ASEAN Insiders: Personal Data Protection*. ZICO Law. Available at: <http://www.zicolaw.com/wp-content/uploads/2016/05/AI-Personal-Data.pdf>

Zimmerman, C. and C. Watts (2004) 'Risks and responsibilities: guidelines for interviewing trafficked women', *Lancet*, 363(9408).