GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

DISRUPTIVE ENDEAVOURS

Ethical guidance for civil society organizations monitoring and responding to online trafficking in endangered species

Alastair MacBeath

FEBRUARY 2022

ABOUT THE AUTHOR

Alastair MacBeath is an analyst at the GI-TOC working within the Observatory of Illicit Economies in the Asia-Pacific with a particular focus on environmental crimes. He is part of the Market Monitoring and Friction Unit, which uses machine-learning technology to research and disrupt the illicit trade in illegal wildlife products.

ACKNOWLEDGEMENTS

The author wishes to thank Gretchen Peters and Marielle Constanza from the Alliance to Counter Crime Online for their insights and contributions. Thanks also go to Carl Miller, Tom Sorell (University of Warwick), Catherine Flick (De Montfort University), David Roberts (University of Kent), Shawn Graham (Carleton University) and Damian Huffer (Stockholm University), who all shared their knowledge and provided feedback throughout the project.

The author would also like to thank Mark Shaw, Louise Taylor and Simone Haysom at the Global Initiative Against Transnational Organized Crime (GI-TOC), as well as the GI-TOC's Publications team. The tool was made possible with funding provided by the government of Norway.

This report was produced in partnership with the Alliance to Counter Crime Online (ACCO). ACCO is a programme of the Centre on Illicit Networks and Transnational Organized Crime, comprising non-profit organizations, academics and citizen investigators who share a commitment to fighting the growth of serious crime on the surface web. They conduct investigations and research into a range of illegal sectors and provide evidence to law enforcement agencies and policymakers with the aim of making the web a safer place.

Cover: © *Suryanto/Anadolu Agency via Getty Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

CONTENTS

Market Monitoring and Friction Unit

The Market Monitoring and Friction Unit (MMFU) is a team within the Global Initiative Against Transnational Organized Crime (GI-TOC) dedicated to monitoring online markets for endangered wildlife species and working towards innovative, effective strategies for disrupting them. The Unit collaborates with civil society organizations and mandated authorities to shut down online illicit wildlife markets.

Websites on the open web – sites that people can access and use every day – host some of the biggest online markets for endangered species.[1] Evidence of wildlife crime is widespread across the internet and private platforms and law enforcement agencies are either unwilling or unable to mount an adequate response.[2]

This mirrors a broader challenge in combating cyber-enabled crime, namely that criminals are on the web, but the police are not. Reasons for this include responses to cybercrime being under-resourced, lack of explicit mandates to address it and the absence of investigatory authorities. This situation manifests unequally around the world. While rich countries have the largest internet-using populations, they also have the most resources to combat online harms. The greatest challenges are found in developing countries, with limited resources for regulating cyberspace or implementing strategies to combat cybercrime.

Within this broader crisis, the online trade in endangered species is easily overlooked, leaving a gap in the global response that allows wildlife traders to openly seek customers online, market goods, conduct transactions and stimulate demand. This contributes to the wider problem of the illicit wildlife trade, which can lead to extinction of species and a heightened risk of outbreaks of zoonotic diseases; it also encourages corruption while enriching highly organized criminal networks.

The MMFU's investigation into the illicit online trade in endangered species grew from the recognition that innovative responses were needed to combat this type of crime. The Unit's aim is to make the open web a space where laws protecting us – and endangered species – are respected in letter and spirit.

With community tools such as this one, the MMFU intends to share its knowledge with the community responding to the harms caused by illicit online wildlife trade. It is hoped that such tools will help to scale the lessons learnt and multiply the number of effective interventions to rein in illicit wildlife markets.

INTRODUCTION

▲ **A yellow-eared parrot – a victim of wildlife trafficking in Bogotá, Colombia.** © *Juancho Torres/Getty Images*

The world's most popular social media platforms, e-commerce sites and specialist forums consistently host advertisements for the sale of endangered species or products made from their parts.[3] These private platforms bear almost no legal liabilities for hosting such content or facilitating this trade, and as a result their responses have been weak and inadequate.

This also complicates the response from law enforcement. Without a clear legal basis to act and being overwhelmed by and ill-equipped to counter online crime in general, wildlife crime is usually low on police forces' priority lists. This lack of prioritization ultimately stems from governments who refuse to acknowledge the urgency of tackling threats to biodiversity or to address the challenges posed by weak responses to cybercrime.

Faced with almost complete impunity for illegal wildlife traders online, civil society actors, including non-governmental organizations (NGOs), conservation organizations and citizen investigators are stepping into the gap: monitoring, reporting, running complex – sometimes clandestine – investigations and even engaging in confrontations to disrupt these illegal markets. But unlike law enforcement, journalists and academics, civil society actors have no universally accepted professional ethical standards or regulations to guide their investigative conduct.

This community tool is aimed at supporting civil society actors in responding to this critical ethical dilemma: how should they balance ethical imperatives to respond to wildlife crime without contravening user privacy, accepted norms related to mass data collection or a platform's terms of service? It also intends to provide an overview of the ethical issues involved in civil society organizations' collection of data, investigation into the illegal online trade in wildlife and possible interventions.

Although this guidance was developed from work researching the online illegal wildlife trade, its findings may be used across a wide range of projects involving the collection of data on the surface web.

The tool is the result of engagements with academics and experts from diverse fields, including ethical research, criminology and information technology. Their experience in researching online vigilantism, scambaiting, online public and private policing, and the policing of the darknet, has been invaluable in highlighting the complex ethical issues confronting those planning to embark on research of this nature.

The guidance document presented here provides an overview of the issue and the circumstances in which it is deemed appropriate for civil society actors to intervene in a domain normally held within the purview of law enforcement. This is followed by a discussion of the ethical challenges arising from the intervention.

For ease of discussion, these ethical challenges have been divided into three thematic areas:

- The ethics of intervention or 'private policing'
- The ethics of privacy and data collection
- Mitigating risks and unintended consequences

Each section presents the ethical questions raised by monitoring and intervention activities and, where possible, provides approaches for assessing and navigating those ethical risks. Organizations conducting projects of this nature should be aware that they may encounter an ethical dilemma for which there is no single correct answer. Therefore, any decision to act should be based on pre-agreed, practical ethics that reflect the real world circumstances of their work.[4]

▲ A monkey for sale in Jakarta. © *Ahmad Zamroni/ AFP via Getty Images*

BALANCING THE RISKS OF ACTION AGAINST THE COSTS OF INACTION

We are in the midst of what is called the 'sixth mass extinction', and we are losing more battles than we are winning in the fight against biodiversity loss. The biomass of wild mammals has fallen by 82%, natural ecosystems have lost 47% of their area and a million species are at risk of extinction.[5] According to the United Nations (UN), this stems from several, often interrelated, human actions: changes in land and sea use; direct exploitation of organisms; climate change; pollution; and invasive alien species outcompeting indigenous ones.[6]

The illegal wildlife trade is tied to both direct exploitation of organisms and the threats posed by invasive alien species. For some species, illegal trade is the overriding threat to their continued existence. To make matters worse, some of these species – such as elephants – have irreplaceable interdependent relationships with many others in their ecosystems. Their absence would therefore lead to further species loss, potentially even triggering regional biodiversity collapses.

The illegal trade in wildlife also poses direct, serious threats to humans. One relates to increasing human contact with wild animals. If allowed to flourish, the illegal trade in wildlife can lead to the outbreak of zoonotic diseases, as seen with avian influenza H5N1, Ebola, severe acute respiratory syndrome (SARS) and HIV. The UN estimates that 75% of all emerging infectious diseases are zoonotic, having been facilitated by environmental destruction and wildlife crime.[7] Current downward trends in protecting biodiversity and ecosystems also undermine progress towards 80% of

the assessed targets of the UN's sustainable development goals, related to poverty, hunger, health, water, cities, climate, oceans and land.[8]

The illegal trade in wildlife is bound up with criminal networks, who commission or organize poaching and harvesting of endangered species, the transport of the resulting commodities and their eventual sale. Some of these networks are highly organized and many are violent. They rely on corruption to function, and the bribery and influence-buying by these criminal networks have wrought havoc on state departments across the world.[9] The work of crucial services such as fisheries and forestry departments, game park management, law enforcement agencies and judicial systems are often undermined to the point where basic regulatory functions decline, even when these were not a direct target of corrupt activities. Wildlife crime is at times also a 'soft' entry point for criminal networks, which hone skills of corruption, coercion, money laundering and logistics in a high-profit crime sector perceived to be 'low risk' owing to weak enforcement.

National and international law enforcement responses to wildlife crime are improving, but they are still seen to be inadequate and hampered by the cross-border nature of these crimes, even when they involve physical commodity flows. However, when the trade moves online – and markets and communications become virtual – it collides with other major law enforcement challenges in the world: the poor global response to cybercrime and the jurisdictional challenges presented by the borderless nature of the web.

This stems, partly, from the poor regulation of companies that provide services on the internet. The internet of today is one dominated by for-profit companies, whose business models rely on their activities not being regulated, opportunities for continuous growth, externalizing the costs of their business practices and, often, surveillance of their users.[10] This applies not only to 'Big Tech' but also to smaller, regionally focused e-commerce and social-media sites, which mimic the business model of large companies but often with even less transparency about their policies, complaints mechanisms or even ownership.[11] The online harms prevalent here span social, political, economic and environmental domains.

Poor regulation and the border-spanning (or border-erasing) nature of the online space crucially undermine the jurisdictional basis for law enforcement. Weak political adaptation to this reality ranges from poor or absent definitions of online crimes in most states to the weak resourcing and skills in cybercrime enforcement units. In addition, investigators face the rise of encryption and privacy-preserving software, technologies which require an entirely different investigatory toolbox.

This situation manifests itself differently around the world. Although rich countries have the largest internet-using populations, they also have the most resources to combat online harms. The greatest challenges are found in developing countries, with limited resources for regulating cyberspace, challenging tech companies or implementing strategies to combat cybercrime.[12]

It is in the midst of this collision – between the threat of wildlife crime and the weak response to cybercrime – that civil society organizations have stepped in to monitor online markets and compile evidence against online traders and platforms facilitating

trade. For almost two decades, civil society organizations have produced reports that record the volume of advertisements found online, the value of goods and the ease of finding illegal or suspect advertisements linked to the illegal wildlife trade.[13] These reports consistently document how the internet has become an important and fast-growing channel for the marketing and sale of endangered species and their body parts.

In addition to their monitoring and intelligence efforts, these organizations have conducted a considerable amount of advocacy work focused on getting big tech companies to act against illegal wildlife traders on their platforms. Thirty-four companies – representing many of the largest social-media and e-commerce businesses in North America, Europe and Asia – have joined the Global Coalition to End Wildlife Trafficking Online.[14] In 2018, the coalition promised to remove, by 2020, 80% of content related to the illegal trade in wildlife (although not formally setting a baseline by which to measure the target). Its members reportedly removed or blocked just under 12 million endangered-species listings as of September 2021. However, without giving independent monitors access to the removed material, and again, without a baseline, it is difficult to access the impact of this intervention.[15] The continued lack of transparency from tech companies and their well-financed efforts to resist legal regulation, together with a knowledge of the genuine difficulty and expense of dealing with the problems, make it seem extremely unlikely that the solution to this problem will come from their self-regulation.

The decision to act

It has become increasingly obvious that neither the voluntary efforts of tech companies nor the (inadequate) enforcement actions of governments have had a significant impact on the illegal wildlife trade online.

Therefore, in addition to our work collaborating with law enforcement agencies and other partners, the MMFU (a team within the GI-TOC) and some members of the Alliance to Counter Crime Online (ACCO) have decided on direct intervention to disrupt online markets. This includes active monitoring, as well as experimental techniques to, for example, decrease trust in traders or get them barred from platforms.

Monitoring illicit online markets and any associated intervention introduce a number of challenges for organizations. The rules of ethical behaviour in the online space are not well defined, particularly when it comes to the ethics of respecting privacy and adopting anonymity. The history of private policing is also fraught with unintended, adverse consequences.

It is in response to understanding such ethical dilemmas, assessing their inherent risks and either avoiding or mitigating them, that this guidance – which the MMFU has applied to its own activities – is produced, to help actors navigate the challenges related to private policing, data collection and privacy, and the associated risks and unintended consequences of monitoring efforts and intervention. This is because the costs and risks of this action must ultimately be balanced against the costs and risks of not intervening.

▲ **Langur infants secured by law enforcement officers from a suspected illegal wildlife trader on Facebook, Riau, Indonesia.** © *Afrianto Silalahi/Barcroft Images via Getty Images*

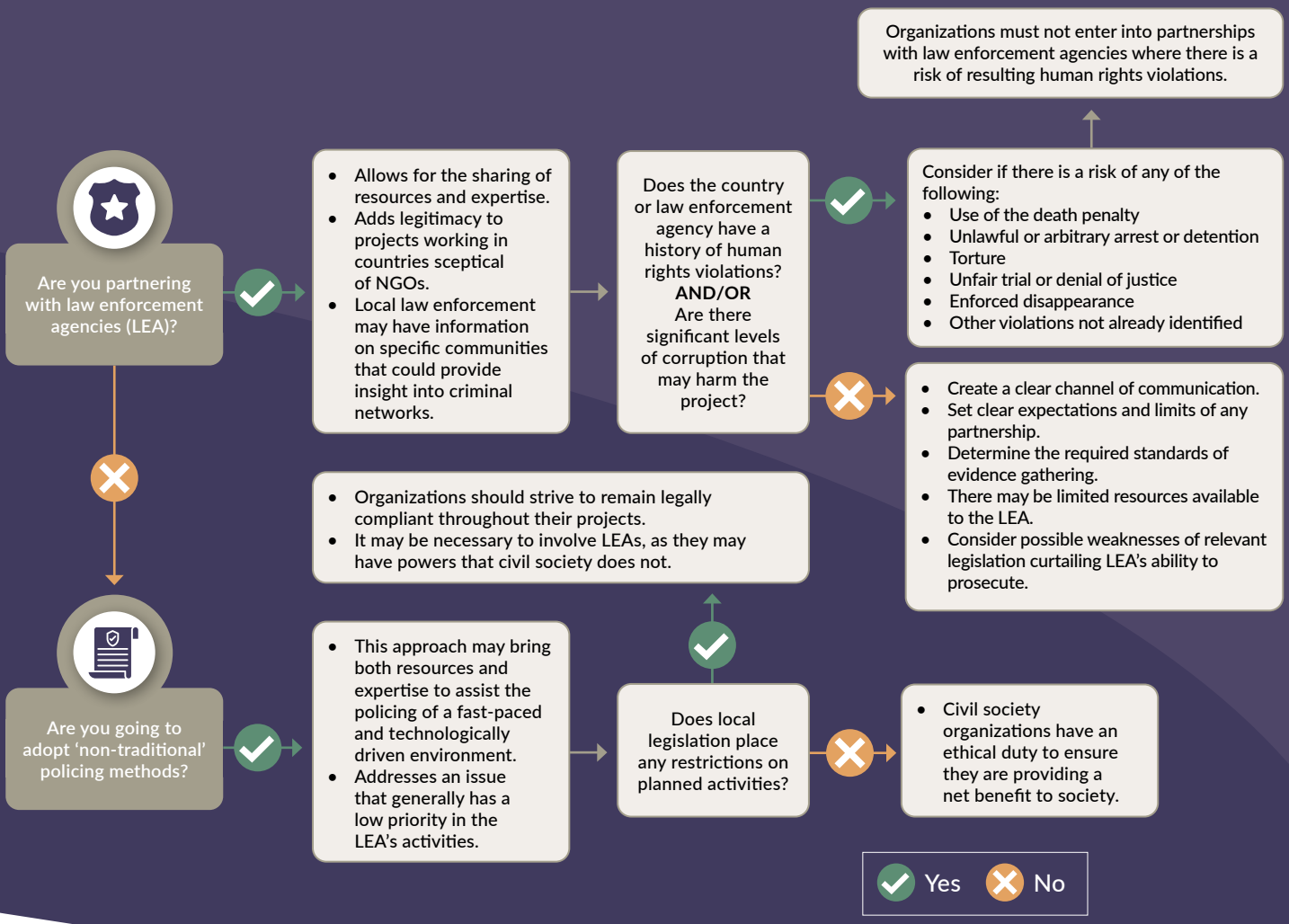
THE ETHICS OF PRIVATE POLICING

The heterogeneity of cyber-enabled illegal wildlife markets presents an obstacle for traditional law-enforcement approaches. In addition to being conducted transnationally, the criminal activity is fragmented based on the language of transaction and the type of product, with a substantial number of networks, companies and sole traders being involved in both licit and illicit trades. This has made it more challenging to identify the markets or actors most worthy of law-enforcement action and raises the cost of regulating the illegal trade in wildlife.[16] This has caused frustration among already under-resourced law enforcement agencies, and the subsequent 'enforcement gap' has resulted in the need for civil society organizations to intervene – typically with disruption tactics.

In the 'offline' world, low levels of police enforcement have driven civil society organizations to adopt more progressive, 'police-like' tactics: engaging in undercover operations, setting up 'stings' to disrupt trafficking, and gathering intelligence that can lead to police investigation, or even evidence for prosecution. In the online space, civil society organizations have largely confined themselves to monitoring, limited covert surveillance and gathering evidence for or directly supporting police investigators. Some organizations are also using active market-friction techniques designed to act as disruptive or preventative policing, or to establish intelligence-gathering traps.

In both the offline and online markets, these approaches raise risks and challenges for organizations acting without legal mandates. Law enforcement agencies' legal authorities, namely powers to enter, search, seize and arrest, are granted through legislation along with the necessary limitations for their use. Without equivalent legal powers, civil society organizations are restricted to tactics that fall within the confines of the legislation of the country in which they are operating.

The decision tree on the following page aims to help organizations determine how ethical considerations will affect the workflow of their project, as explained in the ensuing text.



Partnerships with law enforcement agencies

The nature of cyber-enabled illegal trade in wildlife presents significant, and sometimes insurmountable, challenges for law enforcement agencies, particularly for those operating in countries with poor online infrastructure and weak or non-existent legislation with regard to wildlife trade or operations in cyberspace. It is understood that illegal wildlife traders intentionally operate in countries with weak legislation and enforcement abilities in order to reduce the risk of detection and prosecution.[17] Such safe havens present an effective barrier to law enforcement, and as long as they exist they will be exploited by criminals determined to hamper investigations and avoiding prosecution.[18] Supporting law enforcement to handle these crimes more effectively therefore also involves an ethical rationale.

Partnerships between civil society organizations and law enforcement agencies bring together different skill sets and capabilities, which can produce results beyond what a single organization would have been able to achieve. This has been observed from the partnerships between INTERPOL and organizations such as the GI-TOC, the Worldwide Wildlife Fund and the International Fund for Animal Welfare.[19] Such partnerships allow for a strong and

united front to be formed through sharing resources and expertise required to detect and combat wildlife crime. This simultaneously adds legitimacy to projects in countries whose population may be sceptical of international NGOs, thus alleviating any perception of a foreign agency interfering in the internal affairs of a sovereign state. The detailed knowledge held by local police forces about their communities may include information about the offline element of cyber-enabled crime, which may lend valuable insights into the inner workings of the criminal network.

In contrast, organizations may have an ethical duty that could dissuade them from involving law enforcement agencies or reporting criminal actors to such authorities. Reasons for this may include: human rights violations by a state or known persecution of political dissidents or minorities; a high risk of law enforcement officers alerting criminals to an investigation when there are significant levels of corruption; and when an organization deems an activity to have been wrongly criminalized. However, organizations considering excluding law enforcement agencies or government institutions from projects may expose themselves to criticism and retaliations from the respective governments.[20]

The spectrum of law enforcement agencies is wide, reaching from international bodies such as INTERPOL to local police services specializing in a specific type of crime (e.g. wildlife crime with officers skilled in conservation activities rather than complex cyber-enabled transnational organized crime). The diverse capabilities of these law enforcement agencies (technological, investigative, jurisdictional, etc.) have created a disparity, which means that civil society cannot draw on a uniform or standardized approach to inform their decisions on partnering with law enforcement agencies.

Although there is no overarching ethical imperative to partner with law enforcement agencies, civil society organizations should consider the benefits such a partnership may bring to their projects, while simultaneously being aware of the obstacles that might make such partnerships unworkable. Decisions must be made case by case, informed by the wider value such partnerships would have.

Preventative, disruptive and proactive tactics

Civil society organizations generally prefer to support local law enforcement agencies in investigating and arresting criminal actors. However, understanding the vast challenge that cybercrime poses to law enforcement and the small likelihood of already limited resources being allocated to wildlife crime rather than to human-centric crimes, civil society organizations are also considering other, less-discussed tactics, which fall under the banner of 'policing' strategies.

Traditional policing tactics are broadly aimed at criminal actors' prosecution, although this approach has attracted criticism in some circles because of the costs and time associated with complex investigations that have a small chance of resulting in conviction.[21] Critics note that prosecutions have scant impact in combatting or reducing complex illicit activity, including terrorism-related offences and organized crime. At the other end of the scale sits preventative policing, which aims to block the opportunity for a crime to be committed. More commonly, police employ disruption tactics as an alternative to the time-consuming and expensive cross-border investigations required for successful prosecutions. It has been shown that disruption tactics are often more effective than traditional prosecutions, as they provide flexibility to prevent offences through legitimate means.[22] Such tactics have been defined as a 'flexible, transitory, and dynamic tactic, which can be used more generally to make the environment hostile for the organized crime group … This approach focuses on disrupting the offender's networks, lifestyles and routines.'[23]

Another tactic, which civil society organizations might also adopt, involves 'proactive' policing. An increase in proactive monitoring of online activity has been seen where law enforcement agencies have engaged in illegal activity to gather evidence, for example the FBI and INTERPOL using actual child pornography material on 'trap sites'. Such activity is specially sanctioned and therefore not regarded as a crime, despite its dubious ethical and moral foundations.[24] Civil society organizations do not possess such immunities.

Justification for non-traditional policing techniques by civil society organizations

Precedent exists for private organizations' intervention in online regulation. In addition to traditional law enforcement agencies, a number of quasi-public and commercial organizations have emerged to help regulate the internet, thus creating 'multi-level governance comprising a diverse array of organizations with differing regulatory power'.[25] Among these are NGOs, which have assumed various roles to assist in monitoring the internet. Examples include the Internet Watch Foundation (IWF) in the UK and the Computer Emergency Response Team (CERT) in the US. Both countries have mandated these organizations to monitor the internet for cyber-enabled and cyber-dependent crime and report them to the appropriate authorities or internet service providers for further action.[26] The involvement of NGOs in the monitoring of virtual spaces is part of a wider multilateral approach to online policing that involves different public and private actors in detecting online crime.[27] Such an approach brings both resources and expertise to assist in the policing of a fast-paced and technologically developing environment, which remains a low priority to law enforcement agencies.

The diverse array of tactics being employed in policing online spaces, owing to the involvement of a wide range of organizations, has led to legal and ethical criticism. Although there is no specific legislation outlawing organizations or individuals from monitoring the internet, a number of relevant laws apply (e.g. pertaining to data protection and harassment legislation), and which organizations must observe. The involvement of civil society groups in this regard has also led to growing concerns around their lack of public accountability.[28] Civil society groups embarking on policing projects through detection, reporting and disruption techniques have an ethical duty to ensure that their actions have a net positive effect, in which their tactics are benefiting the wider society and assisting the efforts of national law enforcement agencies as necessary.

Although both IWF and CERT are government-mandated organizations, a large number of organizations involved in online policing act without an official mandate. This, coupled with the lack of push-back from society, suggests that regulation is either not regarded as a necessity or considered too hard to officially enforce. Despite this, organizations should work alongside national law enforcement agencies where possible by alerting them of their intentions and so determine any potential synergies and avoid likely conflicts. This will, among other benefits, open clear channels of communication, leading to increased effectiveness and reduce the risk of civil society groups acting akin to a private police force concerned primarily with its own moral objectives and not those of the country or community where it operates. Civil society organizations must also be aware of the potential limitation to any partnership with law enforcement due to limited funding or political will.

As there are no direct means for the public to hold civil society organizations publicly accountable, organizations should adapt a position of openness through publications detailing their work and successes and by engaging with local media. However, care should be taken to ensure that no harm befalls any researcher or participant. Thus, public engagement and publicity may need to be delayed until after a project has been completed.

Calculated risks: Knowing when to block, blind or bluff

The MMFU has been exploring tactics to intervene in the illegal trade in wildlife with the aim of directly disrupting the online markets. These tactics fit into three broad categories:

- **Platform denial:** The deletion of sellers' profiles or websites through collaboration with social media platforms or internet service providers.
- **Hostile environment:** Making it more difficult for traders to initiate and close transactions.
- **Demand reduction:** Reducing the volume of potential buyers through increased awareness of environmental costs and legal consequences.

In developing these tactics, the MMFU has drawn on the guidance in this community tool to create a matrix (Figure 1) to help identify the ethical considerations, level of harm and the potential risk to the investigation associated with each intervention tactic. These risks include the potential loss of evidence, displacement of criminal activity and harm to staff, and are in addition to the ethical considerations associated with the collection and processing of personal information, as discussed later.

Identifying such risks early assists with implementing appropriate actions. However, it is important to note that it is not possible to accurately predict and successfully mitigate all associated risks and ethical considerations. The MMFU therefore approaches this as a developing process for which there are no easy answers, and so have built ethical checks into its workflow and decision-making. This allows the MMFU to adapt to the changing landscape as its understanding of the illicit online markets develops.

As these tactics are not aimed at punishing those suspected of criminal activities as a court would, but rather to frustrate various aspects of their illicit activity, the MMFU describes only proportional harm suitable for each situation. Such harm may include reporting to law enforcement agencies, the use of disruption tactics to frustrate illicit sales or attempts to influence consumer behaviour to decrease demand, among others. The decision tree on page 7 is useful to help organizations determine the most appropriate tactics. Again, these decision trees are working documents which are adapted as more information about their effectiveness is acquired.

DISRUPTION ACTIVITY	CATEGORY OF DISRUPTION	POTENTIAL INVESTIGATIVE RISKS AND ETHICAL CONSIDERATIONS	HARM LEVEL	RISK LEVEL
Partnership with social media to have seller's profiled deleted	Platform denial	■ Potential loss of evidence if profile is deleted ■ Risk of activity being displaced ■ Increased consumer purchasing motivations	High	Low
Work with internet service provider or relevant agency to have website hosting illegal content deleted	Platform denial	■ Potential loss of evidence if site is deleted ■ Risk of activity being displaced ■ Increased consumer purchasing motivations	High	Low
Leave negative reviews on seller's profile, detailing the illegality of the trade	Hostile environment	■ Accidental targeting of a legal seller ■ Possible accusations of harassment	High	Medium
Distracting sellers with high volumes of requests and questions	Hostile environment	■ Inadvertent stimulation of demand ■ Risk of disproportionate harm ■ Risk of targeting a legal seller ■ Possible accusations of harassment	Medium	High
Flooding problem markets with fake advertisements	Hostile environment	■ Potential harm to the investigator ■ Potential loss of evidence if site is deleted by owner ■ Possible accusations of harassment	Medium	High
Public awareness campaigns targeting a region or country	Demand reduction	■ Identification of sellers through personal information ■ Messaging may conflict with local cultural norms ■ Campaign may have unintended consequences	Low	Low
Targeted advertising in communities at higher risk of being buyers of illegal wildlife products	Demand reduction	■ Targeting could be based on stereotypes or bias ■ Messaging may conflict with local cultural norms ■ Advertising may have unintended consequences	Low	Low
Fake advertisements to attract buyers before alerting them to the illegality of the activity	Demand reduction	■ Entrapment of ignorant buyers ■ Fake advertisements may fall foul of national legislation	Medium	High

FIGURE 1 Example of matrix to help identify ethical considerations, and potential harm and risk.

NOTE: Risk is determined by the likelihood of harm occurring and the possible effect on the investigation. The example shown here should be regarded as for demonstration purposes only.

Terms of service

Organizations must have a detailed knowledge of an internet platform's terms of service before commencing any surveillance or data retrieval activities, to ensure that they remain legally compliant throughout. When dealing with internet and social media platforms with detailed or complex terms of service that outline how and to what extent third parties may access their data, it may be necessary to seek legal advice to ensure compliance. This is especially important if the identification of the relevant jurisdiction is unclear owing to different locations of the civil society organization, the platform's headquarters or the location of the criminal activity.

Although the legal enforceability of online terms of service varies between jurisdictions and depends on how they are displayed, written and agreed upon, civil society organizations with a mandate to counter criminal activity have an ethical responsibility to abide by the intention and spirit of terms of service (within reason), regardless of their legal enforceability. A breach of the terms of service may be ethically acceptable in situations where the terms are specifically designed to hide criminal activities, e.g. a website used to a significant extent for trading in endangered animals. In such a situation, an investigating organization may have an ethical duty to research and report on the illicit activity, although it is again advisable to seek legal guidance specific to the case. It may be possible to use different tactics (e.g. active research techniques rather than web scraping) to access and retrieve the data while abiding by the relevant terms of service.

Depending on the platform or website being accessed, it may be possible to negotiate with the owner or moderator to gain access to data that may otherwise be off limits. During such negotiations, site owners may wish to limit or control access to data and the subsequent narrative of the research.[29] Civil society organizations must balance these requests against their ethical duty and freedom to report the truth. Where internet platforms place unacceptable conditions on the access to data or on its reporting, there is little redress available to civil society organizations other than refusing to agree to the conditions and bringing public attention to the activities of the platform.

© Andrew Brookes/ Getty Images

ETHICS OF DATA COLLECTION AND PRIVACY

The growth in internet use over the past three decades and its global reach has considerably altered the way people's personal data can be accessed by individuals, private companies and governments. This has led to the development of legislation and ethical guidance designed to protect this data, the disclosure of which can result in significant harm to individuals. However, despite legislative advances designed to keep pace with the ever-evolving online world, much of the data protection legislation across the globe is either outdated or non-existent, leaving investigating organizations with little or no legal guidance on the ambit of their access.

This section provides ethical guidance to civil society organizations conducting projects that involve the collection and processing of personal data in jurisdictions with inadequate legislation. It touches on the importance of adhering to legislation and offers broad principles that can be used in context when such legislation is lacking. Readers can also refer to the decision tree on the following page to inform decisions about ethical considerations during data collection.

Although there has been a wide array of guidance published regarding the protection of personal data in academic research, such guidance does not address the issues and complications associated with research into organized criminal networks, where the application of the ethical principles of informed consent and voluntary participation would make the research untenable. Such projects therefore need to strike a balance between the ethical considerations of the individual and the utilitarian benefit such research has for wider society.

ETHICAL CONSIDERATIONS DURING DATA COLLECTION

WHEN COLLECTING AND PROCESSING DATA FROM THE INTERNET, ASK:

Does the country or countries where you are collecting data have suitable data privacy legislation in place?

- ✓ Ensure that you adhere to all applicable requirements.
- ✗ Determine what legislation best takes account of the current challenges of data protection; as of 2022, this is GDPR.

Are there local expectations regarding the use of personal data?

- ✓ Ensure that you adhere to all applicable requirements.
- ✗ Be aware that the lack of ethical expectations does not permit behaviour that would be unethical in another country.

→ Organizations should determine and document a set of ethical standards to be applied equally across the entire project.

Is it possible to obtain informed consent without jeopardizing the project?

- ✓ Obtain informed consent while monitoring any effects this may have.
- ✗ Can it be ethically, practically or methodologically justified to proceed without informed consent?
  - ✓ → Be aware that the needs of the individual must be balanced against the benefit to wider society.
  - ✗ →

Is the information exchange or communication taking place on a public or private space?

- Private → Unless there was an ethical justification not to, organizations will need to obtain informed consent.
- Not sure → **Is the communication taking place in a manner where there is little expectation of privacy?**
  - ✗ → **Are there attempts to restrict membership or access to the online space?**
    - ✓ → Private
    - ✗ → Public
  - ✓ → Public
- Public → The greater the publicity of an online space, the less the expectation of privacy.

Are you using active or passive surveillance to monitor social media or e-commerce sites?

- Passive
  - Ensure that you are familiar with relevant data protection legislation.
  - Consider the legal and ethical implication of a platform's terms of service.
  - Be aware that there is an increased risk of collecting personal data of people not relevant to the project.
  - → Organizations should use adequate technologies and techniques to reduce the risk of collecting personal data from innocent people.
  - Organizations should use fire walls to protect data from theft and security breaches.
  - Where collection cannot be curtailed, the unnecessary data should be deleted. See 2.4
- Active

Are you going to operate in an overt or covert manner?

- Overt
  - Organizations can reveal themselves either to individuals or to website moderators.
  - Be aware that overt research may result in changes of behaviour.
  - Overt research may result in the destruction of evidence.
  - → Organizations should consider the use of virtual private networks (VPNs), aliases or pseudonyms to protect the identities of their researchers.
- Covert

Does the organization require certain details or undertakings to gain entry (e.g. fake photos or phone numbers)?

- ✓ → **Do these actions require committing a crime to gain acceptance to the group?**
  - ✓ → Do not proceed
  - ✗ →
    - Organizations should determine in advance the degree of risk they are willing to endure.
    - Appropriate precautions should be taken to protect the identity of the researcher, including aliases and VPNs.
    - Important! Appropriate resources should be supplied to protect the mental health of the researcher.
- ✗ →

Are you collecting personal data from a country with an oppressive regime or a history of human rights violations?

- ✓ → Note that research data does not enjoy legal privilege and may be liable to subpoena by a court or through government pressure.
  - Organizations should take adequate precautions to protect this data.
  - Determine the absolute minimum amount or type of data required.
  - Use adequate security techniques such as anonymization.
  - Consider holding the data outside the jurisdiction.
- ✗ → Determine in advance the situations where you would be ethically required to disclose information.

  Note: Such disclosures could be made to law enforcement agencies, medical services or through publications to bring public attention to a criminal actor.
  - Disclosure to law enforcement agency. → See section on the ethics of private policing.
  - Disclosure to medical or social services. → Organizations will have an ethical obligation to inform medical or social services to protect an individual from immediate harm.
  - Disclosure intended to 'name and shame'. → Disclosure of personal information can result in harm to the individual owing to the actions of vigilante groups. Organizations may be exposed to legal proceedings, which could result in severe reputational and financial damage.
    - → Organizations should not publish any identifiable information, including telephone numbers or physical or email address. Black out or blur all profile pics, handles, etc.

✓ Yes ✗ No

Legal vs ethical challenges

Globally, following decades of ethical and policy debate about unregulated data capture stemming from the growth of the interconnected online world, legally mandated approaches to data collection are shifting as governments remodel outdated data-protection legislation to keep pace with technological advances. This is worth stating up front, as there is an interplay between the legal regimes governing this area and the debate about the ethics from which it stems. The increasing scope and reach of data-privacy legislation has created a legal framework that sits alongside the ethical considerations associated with the processing of personal data of research subjects.

General data protection regulations: A legal framework based on ethical standards

Since the European Union's introduction of these regulations in 2018, there has been a significant development of data-privacy legislation worldwide, with modern privacy regulations expected to cover an estimated 65% of the world's population by 2023, up from 10% in 2020.[30] This growth in data-privacy legislation has transformed GDPRs from being an exception to being the global standard, subsequently leading to a rise in international privacy regulations and increased public awareness and expectations in matters concerning the use of personal data. Organizations engaging in researching online crime therefore are expected to adhere to a set of practices designed to protect personal data acquired through their projects.

The European Union's regulations require a lawful basis for the processing of personal data. Article 6 outlines six potential bases, namely: consent, contract, legal obligation, vital interest, public task, and legitimate interest.[31] Although gaining the consent of research participants is the ethically desired option, investigators may argue vital or legitimate interest for studies in which informed consent is not possible or advisable. However, such cases would require the investigators to take on extra responsibility to ensure that people's rights and interests are fully considered and protected so that no unwarranted harm befalls the data subjects.[32]

The GDPR framework does allow for the interests of the researcher to outweigh the interests of the data subjects if there is a compelling justification or demonstrable risk. However, owing to the data collection methods typically used in investigating illegal online activity (e.g. web scraping), it is likely that a significant amount of personal data not relevant to the project will be collected. So, although a project would be interested only in data of actors involved in illicit trade, a significant number of others' will be included in the initial set of collected data. It is essential that this data should be disposed of in accordance with the requirements of the GDPR or other relevant data-privacy legislation. The researcher should therefore have a clear and comprehensive understanding of the appropriate data-privacy legislation, as the requirements of the legislation may cover the ethical questions concerning the collection, storage and use of personal data.

The study of transnational crime in cyberspace presents an extra layer of challenge in determining the applicable laws and regulations. For example, data regulations in the countries where investigations are conducted or the illicit actors operate may not be as robust as those where the investigator or institution commissioning the project is based. In this case, it is important to adhere to the standards of the country with the stronger legislative framework while being aware of legislation with extraterritorial reach, as is the case with the European Union's general data protection regulations (GDPRs).[33]

A similar approach is needed when considering the ethical implications of investigations. Researchers do not have carte blanche to collect and process data without considering the associated ethical aspects, even when there are no explicitly stated ethical expectations. Organizations operating transnationally should adhere to a set of written ethical standards that are applied equally across the entire project, regardless of jurisdiction. Such an approach will reduce the risk of bias resulting from different data collection techniques.

Informed consent and voluntary participation

Ethical guidance for academic research projects primarily mandates that a participant must give their informed consent voluntarily and can withdraw it at any time.[34] This requirement is seen as necessary to protect human participants from harm and thus results in the premise that actions for the research lie in the research subject's control.[35] However, such a requirement to gain the informed consent of those involved in illicit activities, including illegal wildlife trade, would be neither feasible nor desirable and any attempt to obtain such consent would present a serious obstacle to the research being practical. It is therefore necessary for civil society organizations conducting research projects of this nature to adopt a more flexible approach to achieve a balance between protecting the research subject from unnecessary harm and utilitarian benefit to the wider society that would be both publicly and legally defensible.

Justifications for not obtaining informed consent

Organizations considering collecting personal data without obtaining informed consent should ensure that they are able to justify the reasons for their decision. There are three justifications for not obtaining informed consent:[36]

- Ethical justifications include situations that have a utilitarian benefit to society and in which the collection and release of information would outweigh the disutility to the individual.
- Practical reasons involve situations in which obtaining consent would make the research impractical.
- Methodological considerations involve the need to disguise the aims of a particular research project to assess a participant's 'real-world' reaction, and as such the participant's informed consent would be gained under false pretences.

Organizations should note that these are not blanket justifications, and that they must always be balanced against the need of both the individual and the wider society while being proportional to the specific case.

Privacy and confidentiality

Expectations of privacy and confidentiality online is subjective and can be different from the expectations associated with offline communication.[37] This results in both practical and ethical concerns for organizations investigating illicit activities, and so it should first be determined whether research subjects have reasonable expectations of privacy before a project that involves data collection is embarked on.

Public and private spaces

Guidance regarding online research has progressed significantly and become more sophisticated, with many institutions, organizations and governments publishing specific research guidance.[38] However, such guidance is always in response to the growth of online platforms and the extent to which significant aspects of human activity have shifted into cyberspace. Unfortunately, there remains scant consensus on how to adapt the ethical definitions for offline public and private spaces to the online environment, although it is generally accepted that less privacy is expected in public online spaces than in semi-private or private spaces. Investigations conducted in public spaces may therefore require no consent from those communicating or exchanging information in these forums.

To determine whether an online space is public or private, the context in which the information exchange or communication takes place should be ascertained.[39] Communication taking place on a self-declared public forum will be associated with few, if any, expectations of privacy, compared with an online forum accessible only to members and who need to confirm their identity through, for example, using a username and password. Such a requirement indicates that members of the forum intend to keep their exchanges private from non-members. This distinction is summarised as follows: 'The greater the acknowledged publicity of the venue, the less obligation there may be to protect individual privacy, confidentiality, right to informed consent, etc.'[40]

Public websites are more likely to exist on the 'surface web' and so it will be expected that they will be detected through passive surveillance techniques, as described later. However, it is more likely that private websites will exist on either the 'deep web' or the darknet and would therefore require active monitoring techniques to gain access. Investigating organizations should be aware that this distinction is not absolute and that they should judge each platform depending on the specific context in which information is exchanged.

Academic standards would mandate that when an organization judges a website or online forum to be a private space, informed consent and voluntary participation of the participants should be obtained unless there was an ethical justification not to. As described earlier, civil society organizations often determine that forgoing informed consent is justified in the course of their work monitoring illicit economies and criminal networks.

Ethics of active monitoring and passive surveillance

Passive surveillance techniques collect data from individuals and entities without their participation in the process, whereas active data collection techniques closely align with more conventional means involving direct interaction between researcher and subject. Organizations looking to monitor social media platforms or e-commerce sites will need to determine whether they intend to use passive surveillance, active monitoring or a combination of the two to achieve their goals.

Data-privacy legislation will likely cover passive surveillance techniques and so organizations should be familiar with the relevant legislation in advance. Owners of websites or social media platforms may also place restrictions on the use of certain technologies to collect data from their applications, which may involve legal and ethical issues outlined in the terms of service (also see 'Terms of service' box).

The use of passive surveillance techniques gives organizations access to a large amount of information that would not be possible using traditional research methods. Such information may directly identify individuals or allow for their identity to be inferred, for example through the use of metadata, which may contain the seller's personal information, geolocation or other unexpected information not relevant to a project.[41] Organizations should therefore take adequate precautions to ensure the collection of only relevant data, and delete unnecessary data from their systems. The retention of irrelevant data presents a risk to both the individual whose data is inadvertently collected and the organization, which may expose them to a liability risk under data-protection legislation.

Active monitoring is a more focused technique and comes with its own set of ethical considerations and associated risks. Organizations considering using active monitoring need to determine whether they will operate in an overt manner by revealing themselves as a researcher – either to individuals or to website moderators – or whether they will assume a covert identity. It is important to note that the use of private groups does not necessarily suggest illegality, just a wish for privacy. For example, there may be private groups for people privately discussing a medical condition they share. Before launching a research project, a researcher ought to consider if the reason for the private forum provides sufficient justification for the use of covert surveillance.

Overt research

If an organization decides to operate in an overt manner, they must consider the resulting changes in behaviour of those present on the platform or e-commerce site. Such changes may present major obstacles to the practicality of the project, as people often use private online forums to discuss issues and engage in behaviour that they are not comfortable sharing in a more public setting. Where illegality is present, there is a risk that participants may either leave the group or move the group onto the deep web to evade further action by law enforcement.

An organization should take adequate precautions to protect the identity of its staff. Where research is conducted overtly, the identity of researchers may be known to the online platform, which may lead to safety considerations for the researcher. Organizations should therefore consider the use of techniques to protect the identities of individual researchers, such as using virtual private networks, pseudonyms, etc., as described later in this document.

Covert research

The use of covert surveillance has a reduced risk for the behaviour of participants operating on forums and websites to change and therefore this type of surveillance increases the probability of evidence being preserved. However, lack of informed consent or explicitly agreed voluntary participation introduces ethical obligations to protect individuals from unnecessary harm and ensure the legitimacy of the research.[42] Organizations that consider using covert surveillance techniques to gain access to private groups should note that certain details or undertakings may be required to gain entry. Therefore, organizations should determine in advance the degree of risk they are willing to take on to gain entry into a group while ensuring they do not cross a legal boundary. Examples may range from participants sharing mobile phone numbers to committing illegal acts to demonstrate that they are genuine.

The holding and disclosure of personal information

The definition of personal information (also known as personally identifiable information) varies between jurisdictions, but for the purpose of this document it is taken to include data that directly identifies an individual or data that, in combination with other information, can indirectly identify an individual.[43] The collection and holding of personal information by organizations are governed by local data privacy legislation and so organizations must familiarize themselves with such legislation to ensure that they are compliant throughout their projects. Organizations conducting research in countries where there are no legal standards regarding data protection should take guidance from legislation that best takes account of the current challenges relating to data protection. As of 2022, this is the EU's GDPR framework.

Safeguarding against the disclosure of personal information

The publication of information that could result in the disclosure, or inference, of an individual's identity represents a potential harm to that individual. Although there are no absolute safeguards against accidental disclosures, it is the responsibility of organizations to mitigate this risk (e.g. through the use of encryption, anonymization and pseudonyms).[44] The potential harms that may result from the loss or abuse of personal data can include

- witnesses being at risk of physical harm or intimidation;
- offenders being at risk of action by vigilantes; and
- compromised police investigations or prosecutions.

Organizations that use computer and machine-learning tools to retrieve data from the internet will have an increased risk of gathering large amounts of irrelevant personal information. As data-protection legislation restricts holding such data to limited circumstances (as with 'legitimate interest' arguments in the GDPR framework), organizations should implement appropriate mitigation measures to restrict collection of such data and, if collected, ensure its timely deletion.

These mitigation measures can include targeting data collection by using specific identifiers, such as geographical locations or certain verbiage, when there is known to be a reduced risk of false positives. When this is not possible, procedures are required to identify irrelevant personal information in order for such information to be deleted.

Organizations operating in counties with oppressive regimes or a history of human rights abuse should take appropriate measures to protect personal information gathered during a project, especially when under pressure from legal authorities to divulge information.[45] It is important to note that research data does not enjoy any legal privilege and so may be liable to subpoena by a court against which the organization will have little recourse.[46] The use of legal routes by governments or other actors to gain access to personal information creates the need for organizations to determine the absolute minimum level of data required to be held in such jurisdictions to meet the needs of the project, along with securing information through measures such as data anonymization. Organizations may also want to consider holding personal information outside these jurisdictions to protect it from court action.

Note that when anonymization is used to safeguard personal information, it is effective only when such information is not held in another form that a government agency or another actor could use to infer the identity of an individual beyond reasonable doubt.[47]

Disclosure and publication of personal information

Before collecting personal information, organizations should determine the situations in which they would be ethically required or justified to release that information. Releasing information could assist with a criminal investigation or prosecution, protect individuals from immediate harm or inform the public of criminal activity.

Organizations releasing personal information to law enforcement agencies to assist with a criminal investigation or prosecution will be both ethically justified and, in many circumstances, required (possible limitations on these disclosures were explained earlier). Organizations similarly have an ethical duty to disclose personal information to medical or social services or another government organization to protect an individual from immediate harm, including human trafficking, child sexual abuse, forced marriage or any situations presenting risk to life.

Although most ethical guidance aimed at academic researchers requires that research subjects give their explicit permission before any identifiable information is published,[48] civil society organizations conducting research and intervention activities aimed at uncovering and disrupting criminal networks have a wider responsibility to society to disclose the identities of criminal actors. Such a disclosure may

be made to law enforcement agencies or through publications to 'name and shame' those inflicting harm on society. Examples can include bringing attention to those who are inflicting harm on the state through criminal activity or corruption.

Organizations that intend to publish personal information for this reason should be aware of the associated risks, both to the individual and to the organization itself, which may lead to criminal prosecution or civil procedures, which could result in reputational or financial damage. There is also the additional risk that police investigations or prosecutions may be compromised due to the release of information.

Before publishing any personal information, organizations must weigh up the wider societal benefits against the risk of harm to the individual, the organization or any ongoing criminal investigation. The necessary steps to mitigate the risk of harm should be taken and legal advice should be sought if warranted. An example of a mitigation tactic is releasing only limited information, with contact information such as telephone numbers and physical or email addresses being kept confidential.

MITIGATING RISKS AND UNINTENDED CONSEQUENCES

▲ Rare animal parts are sold in the wildlife markets of Mongla, Myanmar, on the border with China. *© Ben Davies/ LightRocket via Getty Images*

Research projects involving organized crime are fraught with risks, not only to the researchers but also to innocent bystanders and the criminal actors themselves. Although it is understood that no project can be completely risk free, organizations have an ethical responsibility to identify and mitigate these risks as far as possible. This is achieved through awareness of the potential issues that will be encountered, allowing for their timely identification, proper training of staff and implementing robust procedures to ensure that policies are adhered to throughout the project. For projects that involve inflicting harm to combat harm, it is essential that such actions are proportional and controlled.

The schematic presented on the following page offers useful guidance on how risks and unintended consequences can be mitigated in the project workflow.

MITIGATING RISKS AND UNINTENDED CONSEQUENCES

Guarding against accidental harm

The ethical principle of 'do no harm' is used in medical contexts to guard against interventions that result in a net increase in harm, even when they are intended to alleviate injury or disease. A similar approach can be used in the context of organized crime. When a criminal actor has introduced harm into a scenario, it will be ethically justified to use counter-harm in a proportional and controlled manner to mitigate the harm previously introduced by the criminal actor, thus resulting in a net reduction in harm. In situations where harm has been inflicted intentionally, for example to disrupt criminal activity, those responsible must ensure that their actions are ethical and that as little harm as possible results.[49] However, in situations where well-intended actions result in unintended consequences, those who introduced the harm have an ethical responsibility to undo or mitigate the unintended harm as far as possible.[50]

Inclusion of innocent people

Surveillance and disruption projects run without the informed consent of participants introduce the risk of identifying innocent members of society and who have a reasonable right to privacy. These 'false positives' can be harmful both to the wrongly identified person and to the research project. The organization conducting the project must therefore have robust procedures in place to both guard against such occurrences and minimize harm. There is a substantial risk of this with studies of illegal wildlife trade owing to the close resemblance to legal trade and is further complicated by past reports of illegal products being hidden within legal trades. This may result in the accidental targeting of legal traders wrongly suspected of involvement in illicit trade.

Researchers embarking on projects of this nature need to familiarize themselves with prior research to inform their decisions about effective resource allocation so as to reduce the number of false positives. They should also employ robust checks to differentiate between legal and illegal traders by using known indicators for illegal activity.

Online behaviours adhering to offline standards

The relative ease with which online forums can be infiltrated compared with offline forums, along with the researcher potentially becoming desensitized to the online environment and the associated perceived anonymity, may increase the risk of accidental or deliberate transgressions into either unethical or illegal behaviour. Owing to the lack of physical interaction or contact, those inflicting harm on the other group may become detached from the effects of their actions, resulting in their no longer caring about the resulting consequences.[51]

Although it has become acceptable for law enforcement to access online chat rooms to monitor conversations by assuming the identities of potential victims or criminal actors, there is still the belief that there should be restrictions on law enforcement's ability to intervene indiscriminately in people's online lives.[52] Similar legal and ethical limits exist in online research and therefore it is the responsibility of project leaders to ensure that actors conducting the surveillance and intervention activities are aware of these limits, not only to protect data subjects but to protect the organization and its staff from any unintended consequences, including prosecution.

Protecting staff and vulnerable groups

Reducing the risk of emotional or other harm to staff

In addition to mitigating the risk of potential harm to research participants, project owners have a duty of care to protect researchers and analysts from emotional or physical harm. The growth of social media platforms has highlighted this issue, as their need for commercial content moderators to assess content for compliance with the platform's terms and conditions and community guidelines has exposed moderators to extreme visual content (including acts of lethal violence, animal abuse, hate speech, sexual

abuse and child or revenge pornography).[53] Such repeated exposure over prolonged periods can result in significant harm to the psychological well-being of the researcher.[54]

Although the high-pressure environment associated with commercial content moderation presents distinct challenges that are unlikely in the context of studying illegal wildlife trade, project owners still have an ethical duty to protect researchers by implementing procedures and training to mitigate the risk, increase resilience and provide necessary clinical support when required.

Unless automated systems are in place, risk mitigation will not be able to protect researchers from exposure to extreme content that falls outside the topic of the research.[55] Instead, risk mitigation primarily involves teaching researchers the required skills to deal with such unexpected content and increasing their tolerance, before exposure.[56] People who are highly sensitive to the well-being of animals may not be suited to partake in research where animal cruelty is prevalent owing to the increased risk of emotional harm.

Research into criminal activity is associated with an increased risk of physical violence compared with other research topics. Although the risk of violence is markedly lower in online research than offline research, it is not possible to dismiss the risk of harm befalling a researcher. Appropriate precautions should therefore be put in place to minimize and, if possible, negate the risk of researchers' personal information being disclosed, either accidently or purposefully by a website moderator, to prevent researchers from being identified or located by crime groups.

Figure 2 outlines tactics that the online community has used to inflict harm upon members. The use of personally identifiable information to access websites increases the risk of personal information being released, and so the use of 'burner accounts' with false credentials is advisable.

TACTIC	DESCRIPTION
Doxing	Revealing private information about an individual on the internet.
Dog piling	A group of users coordinate a 'pile on' to harass another user.
Swatting	Making a hoax telephone call to emergency services to have them dispatch heavily armed police to a particular address.
Threats	Death threats, threats of physical violence and threats of sexual violence.

FIGURE 2 Online harassment tactics.

Protection of vulnerable groups

Generating profits through the exploitation of vulnerable people and resources is a characteristic of transnational organized crime. Those embarking on research of this nature will likely encounter people whose circumstances have made them vulnerable to exploitation owing to limited decision-making capacity or limited access to social goods, including rights, opportunities and power. Vulnerable groups include children, the elderly, students, women, prisoners, LGBTQ people, ethnocultural minorities, people with mental health issues and those with diminished capacity for self-determination.[57]

Researchers have an ethical duty to identify vulnerable people partaking in the research, either voluntarily or during the process of covert projects, so that they ensure just treatment of such people during the research process or to protect them from any downstream harms.

In projects in which extremely vulnerable people are expected to be at risk of immediate harm, either from themselves or others, considerations for referral to law enforcement, social workers or another relevant body should be in place.

Reducing risk of cultural bias

The transnational nature of the illegal wildlife trade and the limited resources that may be available for a research project can create the need to focus resources on a specific geographical region. Although it is accepted that no research project can be entirely objective, researchers have an ethical duty to ensure that the rationale used to focus on particular geographical locations or ethnic groups is not based on stereotypes or biases that favour one cultural group or region over another.[58] Decisions must be based on objective research or operational factors, including the location of resources or sources of funding, not subjective opinions about a particular region, country or community, which may result in groups being profiled according to their personal characteristics or backgrounds. Such profiling will expose research projects to accusations of racism and bias and so damage the legitimacy of the organization and associated donors.

Ethical processes and operations

Organizations designing projects that involve disruption tactics must be aware of the danger of inflicting harm with the intent of punishing individuals as opposed to disrupting criminal activity. One way to approach this may be by introducing an ethical code that is agreed to before projects of this nature commence, along with putting in place the necessary structures, thresholds and checklists to reduce the risk of individuals deliberately or accidently overstepping the ethical boundary determined by an organization. In this scenario, any deviation from the agreed ethical code should receive proper confirmation and justification prior to action and such justifications should be recorded in writing for future internal review and archiving.

Adequate reporting processes, along with a culture of openness that encourages feedback, allow for ethical principles to be honed as more information becomes available. Owing to the fast-moving environment and the novelty of the approach, it is important for the reputation of both an organization and the research subjects that decisions around ethical concerns are well considered and not managed in a way akin to completing an administrative checklist.[59] This will allow for theoretical considerations to be moulded into the demands of the real world effectively.

The potential risks and unintended consequences resulting from research of this nature require organizations to take adequate precautions as described here. This is important, as errors and misjudgements can have significant repercussions, not only for individuals but also for projects and organizations, which may suffer reputational damage as a result.

CONCLUSION

▲ A Malaysian customs officer displays red-eared slider tortoises seized after a foiled smuggling attempt by a syndicate. © *Mohd Rasfan/AFP via Getty Images*

The global reach of the online illegal wildlife trade through unregulated cyberspace has had devastating effects on the natural environment, calling for a global response not only from national governments but also from private companies, civil society and individual citizens. An integrated approach involving the use of criminal justice responses, deterrence, preventative measures and disruption techniques is required to counter the growing threat posed by the evolving use of the internet for criminal ends. It is only through such collaboration that we will be able to protect wildlife from criminal actors and create an internet that is safe, fair and supportive of the rule of law. The guidance in this document is aimed at guiding civil society organizations in considering the ethical issues associated with their projects and to prepare appropriate risk mitigation strategies so that, through their resources and knowledge, they can push back against the growing threat the illegal trade in wildlife poses to the environmental, social and economic sustainability of communities.

NOTES

1 Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, Global Initiative Against Transnational Organized Crime (GI-TOC), 2019, https://globalinitiative.net/analysis/in-search-of-cyber-enabled-disruption/.

2 See Katie Paul, Kathleen Miles and Damien Huffer, Two clicks away: Wildlife sales on Facebook, Alliance to Counter Crime Online, 2020, https://www.counteringcrime.org/wildlife-sales-on-facebook; Jo Hastie, Disrupt: Wildlife cybercrime – uncovering the scale and nature of online wildlife trade, International Fund for Animal Welfare, 2018, https://d1jyxxz9imt9yb.cloudfront.net/resource/673/attachment/original/IFAW_-_Disrupt_Wildlife_Cybercrime_-_FINAL_English_-_new_logo.pdf.

3 See Jo Hastie, Disrupt: Wildlife cybercrime – uncovering the scale of online wildlife trade, IFAW, 2018, https://www.ifaw.org/united-kingdom/online-wildlife-trade-2018; Traffic, Stop wildlife crime in the EU – online trade in reptiles and birds in Belgium and the Netherlands, WWF/Traffic, 2020; Felipe Thomaz, Illicit wildlife markets and the dark web: A scenario of the changing dynamics, GI-TOC, 2018, https://globalinitiative.net/analysis/illicit-wildlife-markets-and-the-dark-web/.

4 RM Thompson et al, Ethics and governance for internet-based conservation science research, *Conservation Biology*, 2021, 1–8, https://doi.org/10.1111/cobi.13778.

5 United Nations, Sustainable Development Goals, https://www.un.org/sustainabledevelopment/blog/2019/05/nature-decline-unprecedented-report/.

6 Ibid.

7 UNODC, World wildlife crime report 2020: Trafficking in protected species, UNODC, 2020, https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf.

8 UN Department of Economic and Social Affairs, Transforming our world: The 2030 Agenda for Sustainable Development, UN, 2015, https://sdgs.un.org/2030agenda.

9 Kimon De Greef and Simone Haysom, Disrupting abalone harms: Illicit flows of *H. midae* from South Africa to East Asia, Global Initiative Against Transnational Organized Crime, February 2022.

10 See: Shoshana Zuboff and Karin Schwandt, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019; Amnesty International, Surveillance giants: How the business model of Google and Facebook threatens human rights, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

11 Various ACCO members as well as the GI-TOC have encountered problems with monitoring these tech companies ('middle tech').

12 INTERPOL, Online African organised crime from surface to dark web, 14 August 2020, https://www.interpol.int/en/News-and-Events/News/2020/Online-crime-in-Africa-a-bigger-threat-than-ever-before-INTERPOL-report-warns.

13 For recent reports, see: Katie Paul, Kathleen Miles and Damien Huffer, Two clicks away: Wildlife sales on Facebook, Alliance to Counter Crime Online, 2020, https://www.counteringcrime.org/wildlife-sales-on-facebook; Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, GI-TOC, 2019, https://globalinitiative.net/analysis/in-search-of-cyber-enabled-disruption/; Jo Hastie, Disrupt: Wildlife cybercrime – uncovering the scale and nature of online wildlife trade, International Fund for Animal Welfare, 2018, https://d1jyxxz9imt9yb.cloudfront.net/resource/673/attachment/original/IFAW_-_Disrupt_Wildlife_Cybercrime_-_FINAL_English_-_new_logo.pdf.

14 Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, GI-TOC, 2019, https://globalinitiative.net/analysis/in-search-of-cyber-enabled-disruption/; see also WWF, Coalition to end wildlife trafficking online, https://www.worldwildlife.org/pages/coalition-to-end-wildlife-trafficking-online, for details.

15 Coalition to End Wildlife Trafficking Online, Offline and in the wild: A progress report of the Coalition to End Wildlife Trafficking Online, https://static1.squarespace.com/static/5b53e9789772ae59ffa267ee/t/614c9996d599c17dd162d2b8/1632410006720/Coalition+2021+Progress+Update+2+Pager-English.pdf.

16 Simone Haysom, In search of cyber-enabled disruption: Insights from the Digital Dangers project, GI-TOC, 2019, https://globalinitiative.net/analysis/in-search-of-cyber-enabled-disruption/.

17 UNODC, World wildlife crime report 2020: Trafficking in protected species,2020, https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf.
18 James Wingard and Maria Pascual, Catch me if you can: Legal challenges to illicit trafficking over the internet, GI-TOC, 2018, https://globalinitiative.net/analysis/legal-challenges-to-preventing-iwt-online/.
19 INTERPOL, Environmental crime partnerships, https://www.interpol.int/en/Crimes/Environmental-crime/Environmental-crime-partnerships; also see: ENACT, What we do, https://enactafrica.org/about-us/what-we-do.
20 Tom Phillips, China passes law imposing security controls on foreign NGOs, *The Guardian*, 28 April 2016, https://www.theguardian.com/world/2016/apr/28/china-passes-law-imposing-security-controls-on-foreign-ngos.
21 Mark Button, The "new" private security industry, the private policing of cyberspace and the regulatory questions, *Journal of Contemporary Criminal Justice*, 36,1, 39-55, https://journals.sagepub.com/doi/pdf/10.1177/1043986219890194.
22 S Kirby, H Northey and N Snow, New crimes – new tactics: The emergence and effectiveness of disruption in tackling serious organised crime, *The Journal or Political Criminology*, 1, 1, 33-44, https://core.ac.uk/download/pdf/42138105.pdf.
23 S Kirby and S Penna, Policing mobile criminality: Towards a situational crime prevention approach to organised crime, in Ronald V Clarke, Karen Bullock and Nick Tilley (eds), *Situational Prevention of Organised Crime*, Routledge, 2012, pp 193–212.
24 Tine Munk, Policing virtual spaces: Public and private online challenges in a legal perspective, in Monica den Boer (ed.), *Research Handbook in Common Law*, Bristol: Edward Elgar Publishing, 2018.
25 Adam Crawford, Plural policing in the UK: Policing beyond the police, in Tim Newburn (ed.), *Handbook of Policing*, London: Routledge, 2014, pp 169–170.
26 David S Wall, Policing cybercrimes: Situating the public police in networks of security within cyberspace (revised May 2010), *Police Practice & Research*, 8, 2, 183–205, https://cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.
27 Tine Munk, Policing virtual spaces: Public and private online challenges in a legal perspective, in Monica den Boer (ed.), *Research Handbook in Common Law*, Bristol: Edward Elgar Publishing, 2018.
28 David S Wall, Policing cybercrimes: Situating the public police in networks of security within cyberspace (revised May 2010), *Police Practice & Research*, 8, 2, 183–205, https://cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.
29 University of York, Guidelines for the use of social media data in research, https://www.york.ac.uk/staff/research/governance/research-policies/social-media-data-use-research/.
30 Gartner, Gartner says by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations, Gartner, 14 September 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w.
31 European Parliament, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), article 6, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.
32 Information Commissioner's Office, Guide to the UK General Data Protection Regulation (UK GDPR), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.
33 Organizations should familiarize themselves with the legal requirements of relevant data privacy legislation in the country where they are operating, which may be more progressive than that of their own country, to ensure they meet the minimum legal expectations. They must be aware that data privacy legislation may have 'extraterritorial reach', as with GDPR, which is designed to protect the data of EU citizens when processed both within and outside of the EU. To ensure legal compliance and ease of operations with trans-jurisdictional projects, the adoption of the most developed data privacy legislation across the project may be advisable to reduce the risk of misunderstandings and accidental releases.
34 Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council, Tri-Council policy statement: Ethical conduct for research involving humans, Government of Canada, 2018, p 28, https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf.
35 Paul Spicker, Research without consent, Social Research UPDATE, University of Surrey, p 2, https://sru.soc.surrey.ac.uk/SRU51.pdf.
36 Ibid.
37 Lisa Sugiura, Rosemary Wiles and Catherine Pope, Ethical challenges in online research: Public/private perceptions, *Research Ethics*, 13, 4–4 (2017), 184–199, https://journals.sagepub.com/doi/pdf/10.1177/1747016116650720.
38 L Townsend and C Wallace, The ethics of using social media data in research: A new framework, in K Woodfield (ed.) *The Ethics of Online Research*, Vol. 2, Bingley: Emerald, 2017, pp 189–207; Gabrielle Samuel and Elizabeth Buchanan, Ethical issues in social media research, *Journal of Empirical Research on Human Research Ethics*, 15, 1–2, 3–11.
39 The National Committee for Research Ethics in the Social Sciences and the Humanities, A guide to internet research ethics, https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/a-guide-to-internet-research-ethics.pdf.

40 Charles Ess and the Association of Internet Researchers, Ethical decision-making and internet research: Recommendations from the AoIR Ethics Working Committee, AoIR, 27 November 2002, p 4, www.aoir.org/reports/ethics.pdf.

41 RM Thompson et al, Ethics and governance for internet-based conservation science research, *Conservation Biology*, 2021, 1–8, https://doi.org/10.1111/cobi.13778.

42 ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, https://www.acm.org/code-of-ethics.

43 Information Commissioner's Office, What is personal data?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

44 Social Research Association, Ethical guidelines, December 2003, https://the-sra.org.uk/common/Uploaded%20files/ethical%20guidelines%202003.pdf.

45 A Grinyer, Ethical dilemmas in non-clinical research, *Nursing Ethics*, 8, 2, 123–132.

46 British Sociological Association, Statement of ethical practices, British Sociological Association, 2017, https://www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf.

47 Social Research Association, Ethical guidelines, December 2003, https://the-sra.org.uk/common/Uploaded%20files/ethical%20guidelines%202003.pdf.

48 Charles Ess and the Association of Internet Researchers, Ethical decision-making and internet research: Recommendations from the AoIR Ethics Working Committee, AoIR, 27 November 2002, p 5, www.aoir.org/reports/ethics.pdf.

49 Catherine Flick and Runa A Sandvik, TOR and the Darknet: Researching the world of hidden services, in TW Bynum, et al (eds), *The Possibilities of Ethical ICT*, Kolding: University of Southern Denmark, 2013.

50 ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, https://www.acm.org/code-of-ethics.

51 See Tom Sorell, Scambaiting on the spectrum of digilantism, *Criminal Justice Ethics*, 38, 3, 153–175, https://doi.org/10.1080/0731129X.2019.1681132.

52 Tine Munk, Policing virtual spaces: Public and private online challenges in a legal perspective, in Monica den Boer (ed.), *Research Handbook in Common Law*, Bristol: Edward Elgar, 2018.

53 Miriah Steiger et al, The psychological well-being of content moderators, Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 341, https://doi.org/10.1145/3411764.3445092.

54 Ibid.

55 Indeed, there are utilitarian benefits to exposing researchers to harmful content when the potential results outweigh the perceived harm. See Tom Sorrel, Online grooming and preventative justice, *Crime, Law and Philosophy*, 11, 705–724.

56 Miriah Steiger et al, The psychological well-being of content moderators, Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 341, https://doi.org/10.1145/3411764.3445092.

57 Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council, Tri-Council policy statement: Ethical conduct for research involving humans, Government of Canada, 2018, p 8, https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf.

58 Social Research Association, Ethical guidelines, December 2003, p 18, https://the-sra.org.uk/common/Uploaded%20files/ethical%20guidelines%202003.pdf.

59 RM Thompson et al, Ethics and governance for internet-based conservation science research, *Conservation Biology*, 2021, 1–8, https://doi.org/10.1111/cobi.13778.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net

In partnership with

alliance to counter crime online

www.counteringcrime.org