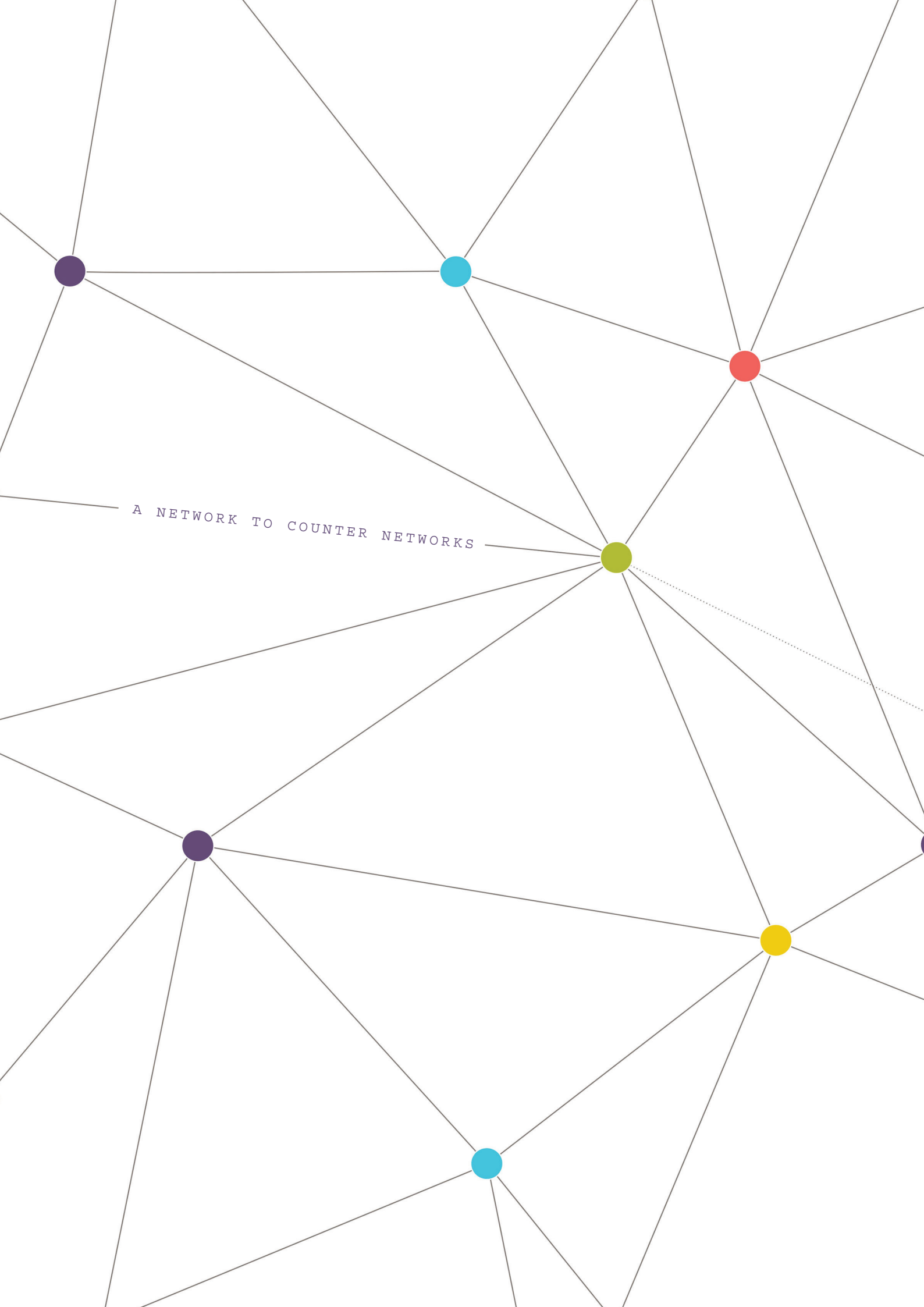
THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

CATCH ME IF YOU CAN

James Wingard and Maria Pascual

Legal challenges to illicit wildlife trafficking over the internet

July 2018


A NETWORK TO COUNTER NETWORKS

CATCH ME IF YOU CAN

James Wingard
and
Maria Pascual

Legal challenges to illicit wildlife trafficking over the internet

July 2018

This policy brief was prepared by Legal Atlas, LLC for the Global Initiative Against Transnational Organized Crime.

Authors: James Wingard, JD, co-founder and legal director, Legal Atlas; Maria Pascual, MSc, co-founder and director, Legal Atlas.

Reviewers: Amanda Rude, JD, senior analyst, Legal Atlas; Simone Haysom, senior analyst, Global Initiative Against Transnational Organized Crime; Tania McCrea-Steele, project lead, Global Wildlife Cybercrime, International Fund for Animal Welfare (IFAW).

Cover photo: iStock/Marco_Piunti

The Global Initiative Against Transnational Organized Crime
WMO Building, 2nd Floor
7bis, Avenue de la Paix
CH-1211 Geneva 1
Switzerland

www.GlobalInitiative.net

Contents

Summary

Although illicit internet trade falls into the larger universe of cybercrime, it is better described as a cyber-enabled crime – in other words, a traditional crime that uses new technologies with the traditional part being the illegal capture of wildlife and the associated physical forms of trade. In addition to the many legal and enforcement challenges associated with conventional wildlife crimes, internet-based illegal wildlife trade (IWT) poses another set of problems for officials, forcing them to operate in a trans-jurisdictional, virtual space that they, and the law, are largely unprepared to manage.

On the practical side, they face substantial difficulties merely distinguishing legal from illegal trade, including:

- knowing which species are involved and which countries' laws apply to the activity in question (e.g. advertising, sale and purchase, arrangement of logistics);
- determining trade quantities and making decisions on whether to invest resources in the pursuit of crimes; and
- knowing which specific legal basis may apply to the species being traded.

In terms of their legal authorities and practices, officials also confront further problems, in that they may have no specific power to carry out covert investigations; no, or limited, access to cybercrime units; and no, or limited, experience with cybercrime laws and digital forensics to conduct necessary investigations.

Concerning the legal frameworks directed at illicit wildlife trade, they face:

- criminal and related laws that do not adequately address all parts of the digital trade chain by expressly criminalizing the advertising of illicit wildlife trade or related offences;
- differing investigative authorities between jurisdictions that compromise transnational enforcement efforts; and
- inconsistent regulation of and limitations to subject matter and personal jurisdiction that create 'digital safe havens' and prevent prosecutions.

Taken as a whole, the overall ability of enforcement authorities to adequately identify, investigate and prosecute the advertising of illicit wildlife on the internet is severely compromised. Key efforts to improve this situation have been included in the conclusion and recommendations to this brief.

Acknowledgements

The authors would like to thank the Government of Norway for funding this report. Digital Dangers forms part of a partnership project between INTERPOL and the Global Initiative Against Transnational Organized Crime, in cooperation with the UN Office on Drugs and Crime.

Key points

- Online IWT poses significant challenges to enforcers, prosecutors and courts. Paramount among these is the difficulty in distinguishing between legal and illegal trade, determining and asserting jurisdiction, and navigating the numerous and often inconsistent laws that apply to cases involving multiple jurisdictions.
- The internet, like any tool, can be both good and bad. Although it makes it easy for people to operate from anywhere, it also allows them to hide their identity and escape detection, defying traditional legal systems that cannot operate when they do not know who and where a criminal is.
- International legislation is urgently needed to take the lead, establishing the basis for harmonization of approaches.
- Within national legislation, there is a concomitant need to carefully examine the applicability of core legislation to determine whether advertising content and the unique aspects of online IWT have been adequately addressed, and whether enforcement officials have the legal tools they need to detect illicit trade and conduct investigations.
- The private sector's critical role in combating online IWT is also a key concern. Strategies must move from ad hoc efforts aimed at forcing illicit trade off certain sites, to proactive protocols with online marketplaces, social-media platforms and courier companies across the board.

Methods

This policy brief draws on three main sources for its analysis. The first is a database of wildlife-trade-related legislation being developed by Legal Atlas soon to be published in its legal intelligence platform. At present, this database includes organized sets of wildlife trade laws for 81 jurisdictions in Africa, Asia, and South and Latin America, and holds legislation relevant to this inquiry from all countries in the world. For this report, legislation from 25 jurisdictions was reviewed and commented on.

In addition to the legislative review, the authors also considered current developments, trends and challenges as discussed by members of the CITES Working Group on Wildlife Cybercrime, of which Legal Atlas is also a member.

Finally, a broad range of articles were reviewed that analyze the jurisdictional challenges of cybercrime generally, as well as the specifics associated with online IWT.

Introduction

To understand the special difficulties presented by illicit wildlife trade activity on the internet, it helps to remember that wildlife law is particularly grounded in geography. Wildlife laws and associated rights often devolve to the smallest jurisdictional unit and, even then, they can be subdivided into smaller parcels.

In many African countries, for example, community-based approaches have been emphasized as a major strategic intervention in hunting management schemes.[1] In the US, wildlife falls within the domain of the state, with each state subdividing hunting units into districts and subdistricts. Germany attaches hunting rights to individual landowners.[2] Even in countries with strong national-level approaches to law, like Mongolia, hunting quotas and management are among the few resources to have a significant local regulatory element. In addition to, or even overlaying these small units, are a wide variety of zones with special rules for wildlife – protected areas, wildlife reserves and special forest zones, to name a few.

For wildlife, the internet takes what is primarily a locally regulated resource and converts it into the object of a borderless crime.

The geography of the law, in this case, becomes unusually important and is really the foundation of everything else. The enforcement of wildlife law operates according to the same legally defined geography, so, for example, crimes are confronted on the ground, with protected areas and forests patrolled by rangers, and the police stopping and searching vehicles, etc.

Determining which laws apply mostly (although not entirely)[3] comes down to a basic geographical question: where did the act constituting the crime occur? International trade in wildlife complicates matters by introducing the possibility of multiple jurisdictions and novel ways of hiding and moving contraband. However, the question as to which laws apply is still primarily a function of the locus of the crime.

The use of the internet as a facilitator of illicit wildlife trade radically alters this situation. While it promotes communication across the globe, it also erases borders and immediately throws into question the basis for establishing jurisdiction for crimes related to the use of the internet. For wildlife, the internet takes what is primarily a locally regulated resource and converts it into the object of a borderless crime.

No longer limited by geographical constraints, cyber-enabled wildlife trade has become yet another major and growing threat to species worldwide. An accurate estimate of the size of the online wildlife market may not be a realistic endeavour,[4] but a number of recent studies provide hints at its magnitude. Conservation NGOs have found thousands of advertisements for endangered species for sale on platforms catering to consumers all over the world. Online wildlife trade is particularly rife in Asia, Europe and the US, and is regionally diverse, with species being offered based on consumer preferences (e.g. live pets in the Middle East, products in China, etc.).[5]

Studies have also revealed that alongside e-commerce sites, social-media platforms, such as Facebook and Instagram, are emerging as popular for marketing endangered wildlife products.[6] Trade on the dark net or dark web, facilitated by crypto-currencies such as Bitcoin, although not considered significant by the other reports in this series,[7] may nonetheless come to play a more important role in the future, further frustrating enforcement by providing even greater levels of anonymity to traders and consumers.[8]

As mentioned, although illicit internet trade is a part of the larger world of cybercrime, it is still considered a traditional crime that is enabled by new technologies[9] – the traditional part being the illegal capture and trade in wildlife. This policy paper for the most part leaves aside the 'traditional' elements, however, to focus on the additional challenges that online trade poses for enforcement agencies. In doing so, it takes the perspective of the investigator faced with determining which jurisdictions and laws apply to the marketed species and the individuals involved in the online transaction (i.e. seller and buyer), as well as the companies supporting it (e.g. market platforms, social media, online payment channels and parcel services). In this, the brief touches on the need for new offence types

and new legal powers for digital evidence collection. The subject, particularly as it concerns questions of jurisdiction, is complex and many of the points discussed are covered only briefly. There is – as of yet – no comprehensive compilation or assessment of how jurisdictions around the world legislate against online trade, and much less how they handle the exercise of jurisdiction in these circumstances.

International legal framework

Because of the transnational and multi-jurisdictional nature of internet-based crimes, INTERPOL stresses the need for a high degree of enforcement interoperability across nations. Consistency in the legal frameworks aimed at combating cybercrime is a foundational principle for such interoperability,[10] and a universal convention to harmonize the operating procedures, rules and legal frameworks is therefore a high priority. The list of international agreements in place that either directly or indirectly apply to international wildlife trade is surprisingly long, including many multilateral and regional treaties, as well as numerous bilateral agreements, and a long list of free-trade agreements.[11] With the exception of one, however, none have addressed the regulatory needs of illicit online wildlife trade.

At present, the only international legal instrument targeting cybercrime in its myriad forms is the Council of Europe Convention on Cybercrime (also known as the Budapest Convention). In force since 2004, the convention has so far been ratified by 57 nations, including most Council of Europe members,[12] as well as some non-members, including Japan, the US, Canada and Australia. Although the convention deals principally with crimes such as copyright infringement, computer-related fraud, child pornography and violations of network security, it also includes new powers and procedures that law enforcers generally need to investigate internet-related crimes regardless of the type. In particular, it provides authorities with harmonized powers to search computer networks, intercept, collect and keep communications data, and it gives authorities augmented seizure powers. Although not specific to illicit online wildlife trade, the Convention on Cybercrime nonetheless provides support for investigating it.[13]

The primary wildlife-trade-related treaty is the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) – the only treaty directed solely at international wildlife trade. It is also among the few treaties that expressly require, and regularly review the adequacy of, national implementing legislation. In 2017, at its 69th Standing Committee, signatories to CITES agreed to track changes in domestic legislation, as well as establish best-practice models, develop enforcement guidelines and engage with online technology companies – all in an effort to combat wildlife cybercrime.[14] This work is in its initial stages and has not yet resulted in changes to practices, compliance requirements or national legislation.

There are a considerable number of other relevant treaties, some of which target e-commerce more broadly. Their primary aim, however, is to protect consumer rights and facilitate cross-border delivery, seeking to foster virtual sales rather than establish a basis for the effective monitoring and investigation of illegal trade.[15] To the extent they promote trade, they may in some instances work against efforts to combat illicit online trade in wildlife. A separate group of treaties provides a basis for international law-enforcement activities for transnational crimes generally. Belonging to this category are the UN Convention Against Corruption and the UN Convention Against Transnational Organized Crime, which, together, provide the basis for harmonizing the national response to crime types that are transnational in nature. Also in this group are the agreements creating INTERPOL and AFRICAPOL, supporting the development of transnational enforcement institutions that have trans-jurisdictional criminal investigative capacity.

National legal frameworks

The adjudication of cases of wildlife trade, including online infractions, depends almost entirely on national legislation.[16] As a whole, the topic has received increasing attention in recent years, resulting in a greater number of national laws with relevant content, and some laws entirely dedicated to it.[17] However, as with the international legal system, most national legal frameworks have yet to respond to the particular challenges posed by transactions made in the global virtual space.

Although each country takes a different approach, a typically wide range of laws regulate wildlife trade.[18] In general, they can be grouped into four major categories:[19]

1. Laws regulating domestic take[20] and trade
2. Laws controlling wildlife uses
3. Laws controlling foreign trade
4. Laws organizing enforcement authorities and powers

The first group, regulating domestic take and trade, sometimes includes a dedicated law on wildlife trade, but more often comprises various laws on hunting and fishing, endangered species, forests or timber, general environmental protection, indigenous rights, transportation and, in a few cases, media and advertising.

The second group, controlling wildlife uses, is wider-ranging, with laws directed at zoos and sanctuaries, traditional medicines, pharmaceuticals, scientific research, captive breeding and agriculture uses (e.g. domestication and use of elephants as draught animals).

The third group, foreign trade in wildlife, focuses on laws on import and export, customs, phytosanitary and quarantine, port authorities and a number of multilateral, regional, and bilateral free-trade agreements.

And, finally, the regulation of law-enforcement authorities and the criminalization of certain acts usually entail organic laws empowering enforcement officers (including rangers, customs and other inspectors, border patrol units and police). This group also includes legislation relating to the criminal code, administrative sanctions laws, environmental liability laws, organized crime, anti-money laundering, anti-corruption and anti-terrorism financing, and firearms. In this last grouping, some countries have legislation related to the organization of the judiciary specific to the environment and wildlife, including environmental courts or so-called 'green benches'.

Despite this plethora of regulation, however, several well-known challenges still remain. Remote and isolated harvesting areas make effective monitoring and enforcement difficult, if not impossible. The ability to conceal illicit wildlife in licit trade chains and the transnational nature of the crime pose challenges to investigators and prosecutors. The inability to identify species prevents customs officers from recognizing and stopping illegal trade. Fines and penalties are sometimes too low to act as a deterrent and do not consistently cover all of the activities associated with the illicit trade chain, leaving gaps in the enforcement scheme. At the same time, trade facilitation measures ease logistics and transport routes for traffickers, while loose market legislation does little to curb increasing demand.

Internet-based wildlife trade merely adds to these existing challenges, and compels enforcement officials to operate in a cross-jurisdictional, virtual space that they are largely unprepared to manage. Lack of access to the product means it is harder to determine the species and legality of the trade, and harder to gather evidence for a case. Often, enforcement rules do not provide the necessary authority or guidance to help agencies confront emerging forms and methods of cybercrimes. Criminal laws do not consider emerging offence types, while limitations to subject and personal jurisdiction hamper investigations and prosecutions. Keeping pace with developments will remain a challenge for the foreseeable future as technologies and cybercrime advance far more rapidly than countries' ability to amend their regulatory frameworks.[21]

Jurisdictional challenges of online crime

Determining criminal jurisdiction (i.e. which country has the authority to prosecute) is a prominent challenge posed by internet-based activities and a necessary starting point in any legal discussion of online wildlife crimes.

The successful prosecution of a crime, whether online or in the real world, ultimately hinges on which jurisdiction has authority over the persons and acts involved, and, therefore, which laws and penalties apply. In any given IWT case, investigators, enforcement personnel and prosecutors must act in concert to establish, at a minimum, the legal status of the item offered, the legality of the transaction or activity (e.g. the advertising, sale, purchase, shipment), as well as to whom liability may attach (the seller, the purchaser, the advertiser, the shipper, an individual, a legal entity), in what form (criminal, civil, administrative) and in what amount. In this sense, jurisdiction is not only the cornerstone of the case, but also the legal piece most challenged by the trans-jurisdictional and veiled nature of internet-based crime.[22]

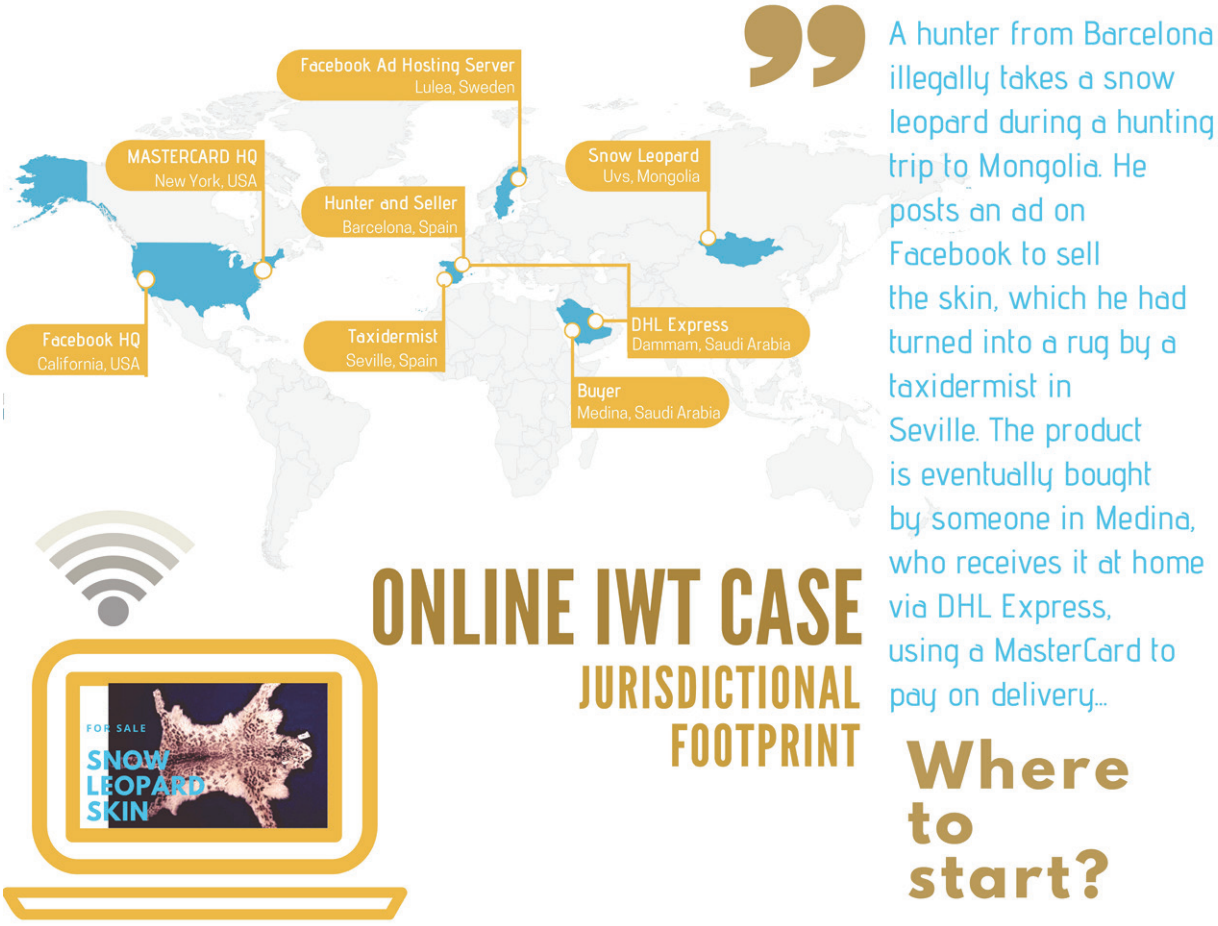
The fluid and physically segregated nature of the virtual environment increases the importance of determining jurisdiction and makes it far more complex.

In a purely domestic wildlife-trade case, jurisdiction would be a function of the 'territorial principle' and settled principally by geographical reference – e.g., where the act constituting the crime occurred.[23] The laws that apply, although there are potentially more than one, would come from this jurisdiction, making investigations and prosecutions relatively straightforward (although not completely free from potential conflicts of law). Transnational wildlife crimes add complexity by introducing the possibility of crimes occurring in separate jurisdictions. For the most part, however, each crime is still tied to a geographical location, with the determination of jurisdiction therefore still a function of the place where the crime occurred.

The introduction of the internet to the transaction erases borders and immediately throws into question the place of the crime and individuals involved, the basis for establishing jurisdiction, and therefore which country has the authority to investigate and prosecute. The criminal conduct may originate from any geographical location. The individuals involved may or may not be nationals of the location where the crime is committed. The species being traded may or may not be from that same jurisdiction, and may or may not be legally traded in the jurisdiction where they are offered or purchased. The online platforms supporting the sale may be headquartered in an entirely different jurisdiction – and different from the one in which the hosting servers containing the evidence may be physically located.

In sum, the fluid and physically segregated nature of the virtual environment increases the importance of determining jurisdiction and simultaneously makes it far more complex: is it the location where the wildlife originates, where the offender resides, the place where the internet address is registered or the location where the effect of the crime is felt (i.e. any place with sufficient ties to the criminal activity)? Is the criminal conduct the online activity itself (the offer for sale, the financial transaction) or that portion of the activity that occurred in the physical world (the possession, the taking of the species and its transport)? Should jurisdiction be decided on the basis of what was done or by the effects of what was done?[24] Is the crime committed in one or all of these places?[25] Figure 1 graphically highlights these complexities.

Figure 1: How should we determine jurisdiction in IWT?



There are further practical and jurisdictional challenges to address when fighting online IWT, discussed in the sections that follow.

The wildlife

An initial challenge is how to determine the country or countries that may have jurisdiction over the animal, part or product, or plant in question. Unlike with other cybercrimes, online wildlife trafficking must leave a footprint both in cyberspace and in the real word.

All illegally traded wildlife originates from a specific location. Similarly, it will be stored, processed, transported, sold, and ultimately consumed or used by some individual in some physical location. Its appearance in the virtual world of online crime is transient, limited to its advertising, arrangement of shipping and payment. When laws do not treat the act of advertising illicit goods as a crime in itself[26] (criminality is still based in part on some real-world aspect, such as the legality of acquisition, possession or transportation), there is a need to reference the laws that regulate the item in the 'offline' environment.

Identifying species and sources

One of the investigatory challenges for online trade is therefore the determination of what the item is, as well as its source and current location. As an initial inquiry, this is not distinct from the prosecution of illegal wildlife trade generally. It is, however, substantially more difficult in an online environment, where the only thing available for inspection is an online advert. In a case of real-world wildlife trading, the item would have been seized, making it possible to identify the species, and sometimes its provenance.

With online trade, however, in the absence of disclosure requirements or the publication of other identifying material, the only information available may be a photograph or written description. With this, it is sometimes possible to determine generally which species is involved,[27] but not necessarily which sub-species and even less likely which national jurisdiction, or sub-jurisdiction (e.g. a community hunting range, game farm or national park) is involved. This knowledge gap is a significant, if not an absolute, impediment to the enforcement of online trade.

When laws do not treat the act of advertising illicit goods as a crime in itself, there is a need to reference the laws that regulate the item in the 'offline' environment.

Knowing generally which species is involved is not good enough to determine which jurisdictions and laws may apply. The range and distribution of many species cross multiple political borders, with their possession and sale potentially implicating multiple legal bases. One of the eight pangolin species,[28] for example, can be found in at least 25 jurisdictions across Africa[29] (see Figure 2). The consumer may be in a number of jurisdictions where it does not occur, with trade passing through several additional jurisdictions. Commercial trade of the animal is theoretically prohibited in all 196 CITES member states.

If the only thing enforcement personnel can deduce is the species name, the only thing they will be able to determine is that the laws of all of these countries may apply, but not which country, and therefore which laws and which penalties.

Determining trade quantities

The quantity being offered or held in possession by the online trader is another enforcement and prosecution consideration easily obscured by the nature of online trade. Unless the seller provides the information, enforcement officials cannot determine the exact quantities of items being offered for sale, or how many more may be in their possession. In some instances, advertisements are deliberately formatted to hide real volumes, giving the appearance of an innocent individual selling a single item.[30] In other instances, traders will state in their advertisements that they can source wildlife on demand; corroborating this, enforcers from the UK's National Wildlife Crime Unit said that they believe some animals were being caught or killed to supply the online demand.[31]

This information gap has a tangible impact on enforcement and prosecution. In most jurisdictions, the amount being offered by or in possession of the trader is directly tied to the penalty level, be it a fine and/or prison sentence. Criminal codes and other laws often use a sliding scale of liability that require the application of higher or lower fines depending on, among other elements, the values and volumes involved.[32] In others, there are minimum and maximum fines, with no express metric for their application but, in general practice, courts will consider the seriousness of the event, including the volume and value.[33]

However, before a case reaches court, decisions must be made by enforcement personnel about whether to initiate an investigation. Enforcement bodies, like any other agency, have financial and human-resource constraints, and will either formally or informally engage in cost-benefit analyses in deciding whether and how they investigate a crime.[34]

Figure 2: Pangolin species naturally occur in 25 legal jurisdictions

The same is true for prosecutors, who are typically given significant discretion over the cases they pursue.[35] While no statistics are available to review the actual impact, it is easy to see how wildlife trade cases, which tend to suffer from a lack of attention and resources in already overburdened courts, are even less likely to be prosecuted if trade quantities cannot be determined in the initial stages.

Knowing the underlying legal basis

Even if a single – or narrower – set of jurisdictions can be ascertained, determining the underlying legal basis for possession and trade still presents a challenge. With the type of information typically offered in an online advertisement, there is only minimal opportunity in this regard.

Some cases are easier, if not perfectly clear. In some instances, determining legality may be a question of a single legal reference. For example, Mongolia's absolute ban on the advertising of very rare and rare species requires only a comparatively simple cross-reference to either the law on fauna (which lists the very rare species)[36] or the Cabinet Ministry's list of rare animals.[37] If the species is on either list, both its advertising and sale are prohibited. For species governed by CITES Appendix I, any offer for commercial sale is most likely in violation of the convention, as well as the national laws of any of the possible source countries. Although this is helpful for some species and products

(e.g. pangolin, elephant ivory, rhino horns, tiger bones, etc.), there is still a possibility the trade could be legal. In Japan, for example, the domestic sale of ivory, other than whole tusks, remains legal and there is no requirement to prove the item was legally obtained.[38]

The global reality, however, is that there is no such thing as an absolute, worldwide ban on the advertising of wildlife. As already mentioned, even for trade in the most protected species, there are exceptions. There are also far more species for which commercial trade is permitted subject to certain conditions. For every one of these species, their legality depends on some combination of how, when, and where they were taken, whether they comply with documentation requirements and the potential end use of the wildlife or product, among other things. If the only information available to enforcement personnel is the minimal data provided in an advertisement, their ability to determine the legal basis of possession and trade is vastly reduced, and in many instances completely eliminated.

The offence

Assuming for the moment that trade in the identified wildlife is restricted in one or more of the possible jurisdictions, the question remains which countries regulate the online activity that has been observed (e.g. sale, purchase, advertising, attempt to purchase) and whether any exceptions or conditions apply that would make the activity either legal or illegal.

Focus on offline offences

Although a global assessment has not yet been conducted, the emerging pattern is that legislation related to wildlife trade is designed to manage 'real world' or 'offline' offences – in other words, the illegal taking, transportation, processing and sale of wildlife. Few countries have legislation concerning online trade, and those that do still tend to connect the legality of its advertising with some other 'real world' requirement. In other words, neither the advertising nor the attempt to purchase online constitutes an offence. Of the 23 countries so far reviewed by Legal Atlas researchers,[39] all of them prohibit the sale of at least some forms of wildlife – typically those with a protected status afforded by a national or international listing (e.g. by CITES).

The US, EU and Australia have, in addition, enacted legislation that prohibits the sale of species that have been illegally obtained, regardless of their protected status.[40] However, only seven of the countries reviewed expressly criminalize the illicit trade of wildlife online – China, Portugal, the Czech Republic, France, Mongolia, Russia and the UK.

Prohibiting advertisements generally

Before discussing the specific criminalization of illicit wildlife advertising, some background on the regulation of advertisements generally is instructive. Advertisements, whether online or in other media, are subject to regulation in every jurisdiction examined in the context of this policy brief, and this is likely to be the case in every jurisdiction in the world.[41] For the most part, these regulations have been developed with the protection of the consumer and market in mind, namely to make sure that the content of advertisements:

- is truthful and fair;
- adheres to standards of public decency;
- does not adversely affect a market; and
- does not promote harmful products.

The object of the regulatory effort is key in understanding its potential application to wildlife trade. A prominent regulatory focus, with the consumer and market in mind, is the prohibition of false and misleading content. In certain instances, the advertising of a particular product or service is banned outright. In Chile, for example, the law prohibits advertising products that are high in calories, sugar, sodium and saturated fats to children under the age of 14.[42] In other instances, advertising a particular product or service is restricted to approved sources. Switzerland, for example, bans the advertisement of lotteries and games of chance that are not operated by cantonal authorities.[43] In other instances, online advertising in all forms is prohibited. The UK, for example, prohibits advertising of prescription-only medicines and applies this to all online ads accessible from the UK – a measure that has reportedly proved useful in decreasing demand, shutting down online pharmacies (through the ISPs), and supporting referrals to foreign enforcement agencies.[44] In these and numerous other examples, the rationale behind such laws is to protect either the individuals or the market targeted by such advertising.

In vanishingly few instances is advertising law concerned with the impact of the advertisement on the resource being advertised or the status of the product. Among the few, but nonetheless consistent, examples of this is the prohibition of child pornography found not only in advertising laws, but also in cybercrime legislation. In this instance, the reason for the regulation is not to protect the consumer, but to protect the children who have been forced into the sex trade. The emerging regulation of wildlife advertising would be another example of this: regulating not for the consumer, but to protect the resource being harmed by trade. As the following section shows, this effort is only just beginning and still faces significant challenges.

In vanishingly few instances is advertising law concerned with the impact of the advertisement on the resource being advertised or the status of the product.

Prohibiting wildlife-trade advertisements

Of the jurisdictions reviewed that expressly criminalize advertising wildlife, only two seem to provide a blanket prohibition: China and Portugal.

China prohibits the 'publication of an advertisement relating to the sale, purchase or utilisation of wildlife'[45] with no further qualification.

Portugal states that wildlife 'may not be advertised or sold through the internet, including portals or platforms, general or specific for this type of sale, even if they are subject to prior registration for users or restricted access'.[46] In both cases, the advertisement by itself is the illegal act and requires no further inquiry into the item's underlying legality. For enforcement personnel, this is a substantial aid in their ability to monitor for and act against illicit trade.

However, looking at these provisions as generic examples of an approach (criminalizing all forms of wildlife advertising), it is still possible to imagine loopholes and challenges. First of all, the provisions themselves have elements that are open to interpretation. What is or is not wildlife, for example, may provide an unexpected loophole:

- Is there a limitation in the definition?
- Does wildlife include both fauna and flora?
- Is it wildlife if it has been domesticated or captive bred?
- Is it wildlife if only a small amount has been included in a medicine?
- What percentage of a product must be composed of wildlife if it is to be deemed a wildlife product?

These types of provisions may also have inherent conflicts with other laws not settled by the text prohibiting the advertisement. What happens, for example, if one law permits the online sale of a product (e.g. traditional medicine or clothing) that the advertising law prohibits? How is this type of conflict of law settled? Is there even a basis for settling conflicts? Finally – and equally importantly for enforcement – the provisions are silent on the question of jurisdiction. Note that the UK's ban on advertising prescription drugs states that illegality is determined based on the jurisdiction from which the advertisement is accessible. This essentially means that an advertisement that is created by an organization outside the UK, but which can be 'accessed'[47] or seen by someone using a computer in the UK, would be governed by UK law. It may be that Portugal and China settle this question through other legislation not reviewed here, but the question of jurisdiction is fundamental to the approach. Each country will have its own framework of laws to consider, but these and other questions will probably still need to be examined to determine legality and effectively enforce against illegal activity.

Advertising predicates

The other jurisdictions reviewed that expressly prohibit online wildlife advertising (France, Mongolia, the Czech Republic and Russia), predicate the legality of the advertisement on compliance with some other legal status (e.g. endangered species status or a hunting ban) or requirement (e.g. obtaining a licence). France's legislation, for example, states that offers for sale or trade of wildlife, whether for free or for a price, through 'all types of medium, including digital … must be subject to the necessary authorizations fixed by an Order of the Council of State'.[48] Mongolia prohibits the advertising of rare and very rare species of fauna and flora (whether online or otherwise), as well as species whose hunting has been temporarily banned.[49] Russia similarly prohibits the online advertising of valuable wildlife, as well as those species in its Red Data Book, which lists rare and endangered species.[50]

Although not yet reviewed, it is possible that other countries have applicable advertising restrictions, even though wildlife is not expressly mentioned. Mongolia, for example, also prohibits advertising when a required licence for a good or service has not been obtained,[51] when the import of an item is prohibited[52] and generally for any goods that are prohibited.[53] Advertising disclosure requirements also include predicates. For licensed goods and services, Mongolia requires the disclosure of the name of the issuing authority, licence and serial number.[54] Predicates are also embedded in the disclosure requirements for CITES trade required by the Czech Republic[55] and the UK.[56]

Whatever form they take, predicates like these are neither unusual in law nor necessarily wrong. However, to the extent they exist, they have a direct impact on the ability to determine legality and act upon it quickly. Predicates basically mean that wildlife advertisements are not automatically illegal. To make this determination, the investigator needs to know what other requirements apply and whether the advertisement complies. In the Czech Republic, for example, the legality of some wildlife trade depends on the status of the species in CITES and compliance with the associated permitting and disclosure requirements.[57] In France's case, the predicate provision does not state the specific requirements and begs the question, what authorizations are 'necessary'? In Mongolia, the question is whether the item advertised is a very rare or rare species, is subject to a hunting ban, requires a licence that has been obtained, is prohibited from import or is a prohibited good.

In all of these instances, determining whether the advertisement constitutes a crime is dependent on the country regulating the item, as well as compliance with the underlying requirements.

Attempt to purchase

In all of the countries so far reviewed that have applicable advertising restrictions, the focus appears to be more on criminalizing advertising, rather than the attempt to purchase or actual purchase. China mentions 'purchasing'

in its law, but actually only criminalizes the 'publication of an advertisement relating' to the purchase. With this limitation, the attempt to purchase, or the actual purchase itself, would not be actionable, unless covered by another law.

Portugal goes a step further, stating that wildlife may not be advertised or 'sold' through the internet. It is not clear, however, whether 'sale' refers to the purchase as well, or an attempt to purchase, and therefore also to the act of the purchaser. In both cases, this part of the trade chain is possibly outside the scope of enforcement.

Even if a law criminalizes the purchase, there is likely to be a need to make sure that what legally constitutes a purchase is further defined to match the kind of activity enforcers are likely to observe on the internet. Does, for example, mere communication or an inquiry count as an attempt to purchase (the activity that may be observed), or is an online payment for the advertised product required (an activity that may not be)? If the internet is only used as a contact point, with all other activity happening offline, will a full payment requirement prevent enforcement? In that same vein, does the product have to be in hand to be considered a purchase; or does the online payment itself qualify as an attempt? These and other nuances will need to be considered as this area of law develops to ensure that criminalization of purchases meets enforcement needs.

It stands to reason that if consumers can act with impunity and continue to openly seek a product, suppliers will certainly find a way to get it to them.

What is clear is that any focus on only one side of the transaction is important both for the loophole it creates, as well as the likely impact on purchasing behaviour that continues to drive illicit trade. In a recent study on wildlife trade in Mongolia, survey results indicate that the criminalization of the seller's act, including advertising, has little impact on the perception of illegality among consumers.[58] With new legislation in place, Mongolia's wildlife traders were far more guarded in 2015 than they were when questioned in 2005. Consumers, on the other hand, still openly discussed their wildlife purchasing habits and participated in the market at activity levels similar to those reported in 2005.[59] It stands to reason that if consumers can act with impunity and continue to openly seek a product, suppliers will certainly find a way to get it to them.

The 'isolated' advertiser

To the extent that laws focus on real-world crimes (e.g. actual possession, illegal take, etc.) and do not criminalize the act of online advertising, or the attempt to sell or purchase online, there is a potential for advertisers to effectively isolate themselves from liability. Advertisers need only claim that they are marketing and neither own, possess, nor are responsible for the taking of the item offered.[60] This defence, as simple as it is, may not act as a complete bar to investigations, but it can make it more difficult to establish the legal basis to open an investigation and obtain a warrant.

In most jurisdictions, there is an obligation on the part of law enforcement to adhere to required search and seizure protocols. One common requirement is that the requesting officer must state the facts giving rise to the belief that a crime is being or has been committed, and describe the place to be searched, as well the persons and things to be seized. An otherwise legal online advertisement that offers no indication of illegality may not be sufficient to meet this burden of proof. The authority to search the place of the advertiser would have to be based on knowledge that the individual has conducted some other illegal act and that a search is likely to produce evidence of such. In sum, failing to criminalize the advertising of illegal wildlife may in some jurisdictions create a loophole that poses a substantial barrier to investigations.

Applicability of cybercrime laws

As with advertising law, the object of cybercrime legislation has an impact on its applicability to wildlife trade. The central focus of cybercrime law is the identification and criminalization of new forms of crime – for example, the various methods of passive and active attacks on computers and computer networks, and to a lesser extent on specific content. In some instances, the new crime types may apply, and to this extent the applicability of cybercrime laws should not be ignored in the continuing debates over legal and enforcement strategies. Where organizations like CITES and governments around the world look to streamline and digitize permitting processes, enforcement records and more, there may indeed be instances when cyber-criminality is the issue. According to one source, 95% of all breached records in 2016 in the US came from three sources – government, retail and technology.[61] In conclusion, if hacking a digital system has value, the chances that it will be the subject of a cybercrime are increasing daily.

For the most part, however, cybercrime laws have only a limited number of content-related offences, and therefore do not automatically address advertising of wildlife. They may nonetheless be applicable to the extent that such content-related offences apply, or treat crimes identified in other laws as a predicate offence if they use cyber technologies. Madagascar's cybercrime law provides an example of a broad predicate offence approach, defining cybercrime as follows: 'The term "cybercrime" means any illegal act committed by means of a computer system or network or any other related physical network or in connection with an information system.'[62]

The Philippines' cybercrime law goes beyond the definition to specifically permit crimes defined in other laws as grounds for its application: 'All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act.'[63]

In the small sampling of cybercrime laws reviewed for this brief,[64] most do not express a predicate offence approach in the same way as the Philippines and Madagascar, limiting their application to the offences listed directly in the cybercrime law, which tend to include a varying collection of offence types directed at illegal access, misuse and disruption of computer systems.

Even the Philippine and Madagascan frameworks fail to make it absolutely clear whether advertising illicit wildlife would be actionable. Madagascar's law may have a broad definition, but none of the offences specifically identified cover advertising content,[65] and further inquiry did not uncover the application of the law outside of the listed offence types. The Philippines' wildlife law, to the extent it is one of the 'special laws' mentioned,[66] may have relevant content. Section 27, in particular, makes it illegal to wilfully and knowingly exploit wildlife or to trade without permission. The application of this provision, however, still depends on the interpretation of whether advertising constitutes either 'exploitation' or 'trade'. The Revised Penal Code does not appear to apply, as it mentions advertising only in the context of trademarks[67] and lotteries;[68] wildlife is mentioned only in relation to the employment of minors as wild-animal tamers;[69] and the sale of goods is criminalized in relation to the misuse of trademarks,[70] prohibited drugs,[71] lottery tickets[72] and human beings.[73]

Athough not currently designed to address illicit wildlife trade, cybercrime laws may nonetheless have some applicability and should certainly be considered in the development of law and enforcement strategies to tackle wildlife crime.

Related financial and logistics offences

In addition to advertising platforms, other online illicit trade enablers include companies providing hosting services, online payment mechanisms, as well as parcel, courier and mail services. Targeting these enablers of online crime can have a substantial impact on enforcement efficiency and effectiveness. Primarily, this narrows the number of enforcement targets (suspects) from many thousands to a limited number of companies.

Financial and logistics facilitators are essentially the bottleneck of illicit trade. While there may be thousands of suppliers and hundreds of thousands of consumers, there can only be so many companies that process payments and move illicit material. Targeting this point in the trade chain therefore has the potential to thwart trade at scales not easily achieved when attempting to prosecute only suppliers or consumers.

Speaking to this improved cost-benefit ratio is the 1999–2001 Operation Avalanche, the largest undercover operation against online commercial child pornography in the US.[74] After detection by the US Postal Service and in partnership with them, enforcers prosecuted a Texas-based company that handled the monthly subscription fee payments (via a post office box in Ft. Worth, Texas, and online credit card payment systems) for a network of more than 5 700 child pornography websites, mostly hosted in Russia and Indonesia. The company's principal owners were charged with 89 counts of conspiracy to distribute child pornography and possession of child pornography, resulting in a life prison sentence for one of them and 14 years' imprisonment for the other. Compared to the enforcement burden of investigating and prosecuting thousands of illegal sites, the identification of the owners of a single company was easy. The search warrant was requested only for one company and the family premises of the owners. After a one-week jury trial, the case was ready for sentencing.[75]

The follow-up to Operation Avalanche highlights the difficulties in prosecuting individual sites and subscribers. This investigation included multiple undercover enforcement operations in the US and 60 other jurisdictions, and was focused on identifying, conducting searches on and arresting child-pornography subscribers. While the total number of subscribers approached 400 000, the number of convictions was vanishingly small. In the US, where there were 35 000 subscribers, only 144 search warrants were issued and, of these, only 120 offenders arrested. In the UK, with 7 000 subscribers identified, numerous challenges and errors during the enforcement operation resulted even fewer convictions. Among the issues that most challenged enforcement officials were the use of IP address masking services, identity-hiding software, claims of credit card fraud by subscribers, and the fact that subscribers visiting the sites may have not downloaded the illegal material and were therefore not in possession of illicit material.[76]

None of the laws that apply restrictions to online wildlife advertising and sales reviewed thus far make any mention of these related parts of the trade chain. However, this does not mean that other laws do not apply and could not already be used to expand the investigations to facilitators of illicit trade, such as conspiracy, aiding and abetting, assisting or concealment of an offender or money laundering. The conviction of the Texas company, for example, was based on the crime of conspiracy to distribute, and not on a provision that targeted payments per se. Most criminal laws in the world include one or more bases for extending liability to other actors involved in a larger criminal scheme, providing a readily available and potential avenue for expanded investigations and prosecutions. The UK, for example, creates the crime of statutory conspiracy (as opposed to common law conspiracy),[77] which applies to any crime, and therefore should apply to online wildlife-trade crimes.[78] The application of these types of provisions is not, however, without limitation. For crimes like conspiracy, successful prosecution would also depend on the ability to prove elements in addition to the crime itself, with agreement between the parties and intent to commit an offence being among the more common.

The offenders

If a crime has been committed, ultimately you need to know who is involved. Regardless of the alleged crime, liability must attach to some person, whether they are a natural person or a legal entity recognized as a 'person' for legal purposes. And no jurisdiction can be asserted over a 'person' without demonstrating to the court that they are subject to that court's authority. Discovering this information is yet another challenge in the range of problems already encountered with internet trade crimes.

Privacy and internet service providers

A full discussion of internet privacy and data-protection laws that restrict what personal information can be held and shared, and their application to wildlife trade is not possible in this short brief. Suffice it to say that the laws that apply are primarily designed to keep personal identifying information private, and most countries have adopted this format. Privacy laws, however, are not absolute in the protections they afford and, as such, present a hurdle, but not an absolute bar to uncovering identities.

The regulation of internet service providers is a major focus in this regard. As a practical matter, users obtain access to the internet through an internet service provider (ISP), with any data they receive or send going through that ISP. The personal information they collect is typically limited to the minimum necessary to provide connectivity (IP address, billing information if applicable, etc.). That said, ISPs do monitor and store information related to each IP address, which can include browsing history and personal information critical to investigations. This practice is referred to as 'data retention' and is subject to varying regulatory approaches across jurisdictions concerning the kind of data that must be kept, the time period for retention, who may access such data, and how.

From 2006, the EU, for example, required ISPs to keep user records for at least two years. There have been some challenges to this however, and it has not yet been adopted by all EU member states, and not uniformly in those that have relevant provisions.[79] As of 2016, Belgium, Bulgaria and Finland all had specifically defined retention periods. Germany, however, is notably against data retention policies, favouring individual privacy protections.[80] The recently adopted General Data Protection Regulation in the EU now requires personal data retention for no longer than is necessary for the purpose for which it was originally obtained. Australia's legislation requires ISPs to hold data for two years.[81] The US does not regulate the retention period, leaving this up to the individual ISPs; although it does require retention once a warrant has been issued and while an investigation or case is active.[82] On the other end of the spectrum, Slovenia's Constitutional Court repealed mandatory data retention in 2014, going so far as to require the deletion of stored metadata.

The same lack of uniformity applies to the warrant requirements to access ISP retained data. As a general rule, personal information held by ISPs cannot be divulged to other private parties without consent, and is usually not available to government officials without formal authorization. The US regulatory approach is an example of this, requiring that a warrant be issued by a court of competent jurisdiction – but 'only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation'.[83]

Even in this instance, a warrant may not be issued if it is against state law, and it may be modified or quashed if the 'records requested are unusually voluminous' or compliance 'would cause an undue burden' to the ISP. The UK, on the other hand, adopted the Regulation of Investigatory Powers Act in 2000, which grants the self-authorized authority to demand the disclosure of ISP data to more than a hundred public bodies, including local authorities, with no external or judicial oversight.[84] Australia has taken a similar approach for a defined set of data, but only allows criminal-law-enforcement agencies access.[85] Given the transnational nature of online wildlife trade, this asymmetrically regulated environment presents yet another challenge to investigators.

Digital surveillance

Digital surveillance is distinct from the standard data monitoring that ISPs may conduct; it refers instead to the gathering of information on individuals by tracking their behaviour when using the internet. Compared to covert surveillance operations in the real world, digital surveillance offers a very cost-effective, fast and safe opportunity to gather digital evidence. In this regard, however, a note of caution should be given considering the larger legal and

human-rights-related implications of digital surveillance. As noted by Sadoff in his 2016 article, 'Bringing fugitives to justice', 'The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent internet users.'[86]

Organizations such as Privacy International and the Electronic Privacy Information Center developed a world map of surveillance societies, rating various nations for their civil-liberties record. The study raises red flags for what are considered the most 'endemic surveillance' societies (including the US, UK, Thailand, Taiwan, Singapore, Russia, China and Malaysia), and points to the fact that citizens are vulnerable for misuse and abuse of their digital information when surveillance technology develops faster than legislation.[87] The UK, for example, grants broad authorities to engage in all forms of surveillance, including covert surveillance.[88] The UK police can also download digital data from a cellphone without a warrant.[89] Poland has included a specific provision in its 2016 amendment to the Police Act,[90] extending the surveillance authority to 'internet data'. This broadens the current competences of enforcement and intelligence services to encompass metadata concerning citizens' activity on the internet. Digital surveillance, in other words, is becoming a standard, if not universal, practice.

Digital surveillance is becoming a standard, if not universal, practice.

International conventions fall short in providing clear guidance on this controversial issue. Both the UN Convention Against Transnational Organized Crime (Art. 20) and the UN Convention Against Corruption (Art. 50), although calling for the development of digital forensic techniques, do not establish clear principles or guidelines for them.

Identity fraud and VPNs

Perhaps most problematic for the investigation of online crimes is the growing use of false IDs, virtual private networks (VPNs) – used to mask a user's IP address – encrypted communications protocols (used in most social-media platforms), as well as password locks in computers and mobile devices. It is these methods, rather than the privacy rules surrounding ISP services and tracking internet users that create an environment of anonymity and most hamper enforcement efforts. Only the first two of these methods are reviewed in this policy brief.

False IDs and VPNs are a major concern for law enforcement, as they constitute a growing and easily accessible method for hiding identity. In addition to masking true identities, a good VPN service will typically include three additional tools or services. The first is a no-logs policy, which is the promise to keep no records of personally identifying information; the second is the use of shared IP addresses. As multiple users have the same ID, it becomes impossible for those tracking activity to know which activity belongs to which user. And finally, the use of anonymous payment methods (e.g. PayPal, Bitcoin) makes it possible to conduct financial transactions with the same security.

For the most part, VPNs are legal. Only 10 countries ban or severely restrict their use. For five of these, only government-approved VPNs are allowed and require terms that effectively defeat the identity-masking function of the service – China, Russia, Iran, UAE and Oman. In the other five, there is a complete ban in effect – Turkey, Iraq, Turkmenistan, Belarus and North Korea. In the remaining jurisdictions of the world, VPNs appear to be legal[91] and by all accounts a rapidly growing service sector.

Despite the privacy protections they afford, VPNs are not a complete cover for illegal activity. They are intended to maintain privacy for legitimate personal and business reasons, and not to act as a shield for crime. As a matter of general criminal law, there is no argument that law enforcement agencies could not access any VPN retained data in the same way they access ISP retained data, with or without data retention requirements. Indeed, some jurisdictions may in fact require data retention (e.g. Australia).[92] However, even though not yet mandatory and despite claims to the contrary, some VPNs do monitor and retain data,[93] and, of course, they cannot operate outside the law. Pursuant to a valid warrant, it is likely that the logs they do have can be obtained by law enforcement and

used in a criminal investigation. Furthermore, failing to cooperate with such a warrant would normally expose them to criminal liability for obstruction, conspiracy, aiding and abetting, or other similar charges. The use of VPNs is, nonetheless, problematic for law enforcement, to the extent they may not be subject to the same data retention requirements as ISPs. The push for stricter data retention requirements by ISPs is in fact considered a major driver for observed increases in VPN subscriptions.[94]

Establishing personal jurisdiction

Once the individuals responsible for suspected wildlife-trade crime have been identified, it is still necessary to determine whether a country can exercise jurisdiction over them personally. Before a court may decide a case, in addition to determining whether it has jurisdiction over the subject, it must also determine whether it has jurisdiction over the parties involved. The basic tenet is that a person may not be prosecuted in a foreign jurisdiction unless he or she has established some relationship with that forum that would lead them to reasonably anticipate being sued there. In the case of internet trade, it may be true that a person has committed an act that constitutes a crime in Country A, is a citizen of Country B, where it is also a crime, but who resides in Country C, where it is not a crime. It is not automatically true that either Country A or B can be called upon to hold the individual liable for the act. With the exception of crimes for which universal jurisdiction applies, courts cannot claim jurisdiction over everyone in the world for any crime, including over their own nationals when they are in foreign jurisdictions.

With respect to personal jurisdiction, there are few bright lines in this analysis and none of them apply directly to wildlife trade. Pursuant to international principles of jurisdiction, courts may prosecute anyone for revealing national secrets, falsifying official documents, or inciting war, torture or genocide.[95] As these activities threaten national security no matter where they are committed, international jurisprudence considers it appropriate for any nation to exercise jurisdiction. In this sense, they are 'universal offences' and may be prosecuted extraterritorially by any nation, regardless of the citizenship or location of the individual.[96]

For wildlife-trade crimes, however, a court's authority to establish personal jurisdiction is more limited and more complicated. No matter how well founded the interests may be (e.g. the need to prevent illegal trade in an endangered species), the principles of sovereignty advocate for a moderated approach to the exercise of extraterritorial personal jurisdiction.

Jurisdiction based on effect

One of the trends in personal jurisdiction in response to internet-related crimes is the use of the 'effects' test, whether created by judicial opinion or as a function of statutory law. This test essentially allows a court to assert jurisdiction over a person because their actions have an 'effect' in that jurisdiction – basically some level of business or personal activity in the jurisdiction, or to consent to the jurisdiction of the country. In the US, the elements used to establish an effect include a determination of whether the person (or legal entity)

- has consented to jurisdiction by act;
- has in the past done business, or regularly carries on business in the jurisdiction;
- has engaged in activity outside the state, but which has a substantial, direct, and foreseeable effect within the state; or
- the thing that is the subject of adjudication is owned, possessed or used in the state.

In other countries, this type of jurisdiction is a function of statutory law. In the UK, for example, more than one statute makes advertising particular content in the internet a crime judiciable in the UK if the advertisement can be

accessed in the UK, regardless of where the advertiser resides.[97] The event triggering jurisdiction is the accessibility of the website, and the justification is based on the 'effect' the advertisement has in that jurisdiction.

Malaysia's cyberspace law similarly extends to offences committed by a person, regardless of their nationality and residence, if the computer, program or data was either in Malaysia, or capable of being connected to or sent to or used by or with a computer in Malaysia.[98]

Nigeria takes a more restricted approach in this regard, limiting jurisdiction for cybercrimes to instances where the victim of the offence is a citizen or resident of Nigeria, or where the offender is physically present in the country.[99] Under this construction, the mere presence of an advertisement that has not caused harm to someone in Nigeria is likely not sufficient to extend jurisdiction.

The Philippines goes even further in restricting this jurisdiction, allowing prosecution only when the crime is committed by a Filipino national (regardless of where the crime was committed) or by an individual physically present in the country.[100] The impact on the victims, in this instance, does not constitute grounds for the extension of jurisdiction. In all instances, personal jurisdiction is based on some relationship between the accused and the prosecuting country, but the relationship that triggers this jurisdiction differs between countries.

A full review of how this type of jurisdiction is used across the globe, and how it applies specifically to the IWT has not been completed. To the extent it follows the UK and Malaysian examples, its usefulness to law enforcement for internet-based crime is its ability to remove geographical barriers to personal jurisdiction in the same way the internet removes boundaries to doing business. However, this usefulness is also a reason courts in the US at least seek to limit its application. In the US, the Zippo case limited jurisdiction to instances where the defendant either actively marketed a product or the website had a degree of interactivity that suggests the website seeks to do business in a particular forum.[101] Under this reasoning, a passive website, where information is merely posted, would escape liability.

There have been numerous other cases in the US, some allowing personal jurisdiction for more passive acts of advertising with no interactivity or explicit targeting of a jurisdiction. This area of law is still evolving and a final analysis of its application across a broader landscape has not been completed.

Dealing with safe havens

A related problem, and a natural consequence of the internet, is the flexibility it affords traders in the selection of their jurisdictional seat. For criminals, it offers the opportunity to avoid countries with strong cybercrime legislation, the digital equivalent of a law-enforcement 'safe haven'.[102]

In this context, a safe haven is any jurisdiction that provides legal protection for those within its geographical control 'while they carry out unlawful operations and/or evade the reach of external law enforcement'.[103] With respect to wildlife trade, the concept might be more specifically defined as any country that either does not recognize online wildlife trade as a crime, or that legally allows online trade in a particular species or part, and that does not recognize the extraterritorial jurisdiction of another country where such trade is illegal. The combination is an effective barrier to enforcement and, so long as such safe havens exist, the protection they afford will be exploited, hampering investigations and preventing adequate prosecution.[104] Preventing them is therefore another major jurisdictional challenge.

Conclusion and recommendations

Essentially, there is a mismatch between the borderless and veiled nature of crimes committed on the internet and the jurisdictional limitations inherent in legal systems. While criminal networks operate at scales that regularly cross and ignore sovereign boundaries, law-enforcement officials and the courts cannot. Legal systems are an expression of a geographically defined sovereign state and therefore mostly bound by its geographical limits. Even in instances where a country extends its jurisdiction to crimes committed on foreign soil, it still applies the laws of its jurisdiction to those individuals subject to its jurisdiction.[105]

There is a mismatch between the borderless and veiled nature of crimes committed on the internet and the jurisdictional limitations inherent in legal systems.

Likewise, when extending jurisdiction to foreign nationals, there must be a sufficient nexus with the prosecuting state: either the foreign national is physically present in the state or has sufficient dealings with the state such that he or she can be considered subject to its laws.

Sometimes this is expansive and applies to anyone, regardless of their nationality and residence (as is the case in the UK and Malaysia). In others, however, it is limited to the nationals of the prosecuting country (e.g. the Philippines).

Of course, trans-jurisdictional questions have been an issue in the past. But if they were difficult when trade was almost entirely a real-world event, they have become a paramount issue in the digital world. While the internet makes it easy for people to hide their identity and operate from anywhere, the legal system cannot operate if it does not know who and where they are. This reality has allowed internet-based crimes of all types to flourish, including online IWT.

International legislation

International legislation is urgently needed to establish the basis for harmonization of approaches. Not discussed in any detail in this brief, the following points have nonetheless been identified as key:

- As noted in the Introduction, the current Cybercrime Convention only has 57 signatories, and leaves out key jurisdictions and crime types, including online wildlife trade.
- Already identified by the CITES Wildlife Cybercrime Working Group, there is the need and an opportunity to develop a new CITES policy – whether in the form of a chapter, amendment or protocol to criminalize specifically the online advertising and sale of Appendix 1 species, and to amplify disclosure requirements for Appendix II and III listed species.
- In support of international enforcement efforts is the need to develop and roll out the INTERPOL wildlife cybercrime enforcement guidelines. Coupled with this would also be an international database of online wildlife crime fed by all jurisdictions based on a standardized reporting protocol, supporting improved understanding of crime patterns and species targeted.

National legislation

While international efforts are critical, day-to-day enforcement and prosecution remain a function of national jurisdictions and must be a major focus. At this level, there is first and foremost a need to carefully examine, at a minimum, the applicability of a core set of existing laws to determine whether advertising content and related

parts of the wildlife trade chain have been adequately addressed. These may include the following:

- Advertising laws
- Criminal codes
- Criminal procedure codes
- Rules of evidence
- Cybercrime legislation
- Wildlife-trade-related legislation
- Laws related to covert operations and investigations

The review and analysis must also be conducted to match the scale of the problem, which, given the nature of the internet, is global.

From the limited research conducted for this policy brief, it is already known that there will be various approaches and that inconsistencies will continue to present challenges both nationally and internationally. Coupled, therefore, with a mapping of applicable legislation there would need to be the distillation of best practices and the identification of key components that:

- harmonize investigatory authorities and evidentiary processes;
- include offence types that target all parts of the trade chain in the digital environment (e.g. advertising, offer for sale, actual sale, purchase, attempt to purchase, facilitation);
- provide enforcement authorities with the necessary powers and guidelines to act appropriately in the digital environment;
- ease enforcement and monitoring burdens by, for example, amplifying registration and disclosure requirements for wildlife trade of all types, identifying the location and identity of traders and buyers, as well as the identify and legality of the item being traded;
- prevent the use of digital 'safe havens' that allow illicit wildlife traders to act with impunity; and
- provide prosecutors with the legal basis to bring cases against traders based on digital evidence alone.

Some of the challenges currently faced may be eased simply through better understanding and use of existing legal foundations. Training of investigators, prosecutors and judges in this regard will of course be required. However, as this brief already highlights, the legislative gaps are significant and will require a concerted, long-term effort to change. Programmes to upgrade, document and monitor legislation developments are therefore also urgently needed.

Private-sector engagement

Private actors, such as ISPs, online financial mechanisms and logistics services have appeared as key enablers of online wildlife crimes. Compared to the number of traders and buyers, these private-sector actors are relatively few in number. As enforcement actions in the past have already shown, engagement with the private sector in monitoring and preventing illegal trade can be a cost-effective approach.

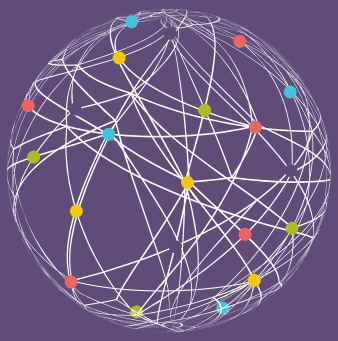
Strategies so far have focused on getting the technology sector to force illegal transactions off their sites and coordinate with enforcement efforts. There remains an urgent need, however, to establish protocols with online marketplaces, social-media platforms and courier companies across the board, and not on an ad hoc basis.

Notes

1. GR Damm, Recreational trophy hunting: 'What do we know and what should we do?', in RD Baldus, GR Damm and K Wollscheid (eds), *Best Practices in Sustainable Hunting – A Guide to Best Practices from Around the World*. CIC (International Council for Game and Wildlife Conservation), 2008, pp 5–11. The authors note that '[o]n communal land, trophy hunting is a key component of community conservation schemes in several countries, including Botswana, Central African Republic, Namibia, Tanzania, Zambia and Zimbabwe'.
2. As regulated by the Bundesjagdgesetz, 1976 and the laws of the Länder.
3. This discussion is deliberately simplified for the purposes of this comparison. There are numerous complexities in the application of law even within a single jurisdiction that also present challenges to enforcement and prosecution.
4. There is no consensus on the economic value of the illegal wildlife trade, or that portion facilitated by the internet. Estimates range from $15 billion to $150 billion annually, depending on the source and method of assessment. See, for example, *UNEP Year Book 2014*, Emerging issues update: Illegal trade in wildlife – US$50–150 billion; UNEP's Illegal trade in wildlife factsheet, May 2016 ($15–20 billion); meanwhile TRAFFIC estimates the trade at between $24.8 and $40 billion (see http://www.traffic.org/trade/).
5. Environmental Investigation Agency, Humane Society International, Blood e-commerce: Rakuten's profits from the slaughter of elephants and whales, March 2014, https://eia-international.org/wp-content/uploads/Blood-e-Commerce-FINAL.pdf; see also J Hastie and T McCrea-Steele, International Fund for Animal Welfare, Wanted – dead or alive: Exposing online wildlife trade, 2014, https://www.ifaw.org/united-states/resource-centre/wanted-dead-or-alive-exposing-online-wildlife-trade.
6. Ibid.
7. S Haysom, Digitally enhanced responses: New horizons for combating online illegal wildlife trade, Global Initiative Against Transnational Organized Crime, May 2018, http://globalinitiative.net/wp-content/uploads/2018/06/TGIATOC-Digital-Responses-Report-WEB.pdf; see also R Horsley. Cut the purse strings – Targeting the online illegal wildlife trade through digital payment systems, Global Initiative Against Transnational Organized Crime, May 2018, http://globalinitiative.net/wp-content/uploads/2018/06/TGIATOC-Purse-Strings-Report-.pdf.
8. International Fund for Animal Welfare (IFAW)/US Department of State/AWF, Illegal wildlife trade in the darknet, INTERPOL News, 2017, https://www.interpol.int/News-and-media/News/2017/N2017-080.
9. IFAW, Caught in the web: Wildlife trade on the internet, 2005, https://www.ifaw.org/united-states/resource-centre/caught-web.
10. INTERPOL Global Complex for Innovation (IGCI), National cyber review project sheet, March 2017, https://www.google.co.za/search?ei=c68nW76mAuGMgAbs3YzYDw&q =INTERPOL+Global+Complex+for+Innovation+%28IGCI%29%2C+National+cyber+review+project+sheet&oq.
11. Among these are the Convention of Migratory Species, the Convention of Biological Diversity, an abundant group of trade-based agreements at global, regional and bilateral scales, many of which include common phytosanitary standards and harmonized custom procedures intended to improve international trade in goods, including wildlife. Trade agreements include those promoted by the World Trade Organization and the World Customs Organization, both under the umbrella of the UN. Across the Americas, the regional trade agreements of NAFTA, ALCA, Mercosur, CARICOM and the Central American Common Market are the more relevant ones. The EU and the ASEAN groupings have created free trade areas in Europe and Asia. Lastly, the African Union and geographical regional organizations, such as SADC, ECOWAS, ECCAS and UMA, have their own treaties and protocols directed at the liberalization and harmonization of trade.
12. It has not yet been signed by the following Council of Europe members: Russia, Sweden, Ireland, Romania and San Marino.
13. IFAW, Caught in the web: Wildlife trade on the internet, 2005, https://www.ifaw.org/united-states/resource-centre/caught-web.
14. Summary record, CITES 69th Meeting of the Standing Committee, Geneva, 27 November–1 December 2017, https://cites.org/sites/default/files/eng/com/sc/69/sum/E-SC69-SR.pdf.
15. An example is the EU Directive on E-Commerce, which defines the European framework for online services, including online advertising and sales. It establishes harmonized rules for transparency and information requirements for online service providers, commercial communications and electronic contracts. It also establishes limitations for the liability of intermediary service providers and bans member states from imposing any general obligation on internet service providers to monitor the content they manage. See https://ec.europa.eu/digital-single-market/en/e-commerce-directive.
16. The application of international law in national jurisdictions is a complex subject, but in general, most jurisdictions require the incorporation of treaty obligations into national law before a court will recognize them.
17. See, for example, Cameroon's Decree No. 2005/2869 / PM OF 29 JULY 2005: Fixing the detailed rules for the implementation of certain provisions of the Convention on International Trade in Endangered Species of wild Fauna and Flora.
18. Legal Atlas has identified at least 43 different types of legislation used to regulate wildlife take and trade across more than 160 jurisdictions covering numerous trade types, such as hunting, trapping, domestication, captive breeding, zoological uses, transportation, possession, medicinal uses and others.
19. These categories are based on independent research conducted by Legal Atlas to compile a global database of wildlife trade laws.
20. As used in this context, the term 'take' refers to a broad range of activities that are often identified and regulated as separate concepts in law, including, for example, hunting, trapping, netting, driving, etc. It is considered a more useful term here, as it would encompass all laws that address one or more of these activities.
21. M Gencke, Understanding cybercrime: Phenomena, challenges and legal response. UN International Telecommunications Union (ITU), November 2014, https://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
22. Kim Soukieh, Cybercrime – The shifting doctrine of jurisdiction, *Canberra Law Review*, 10, 1, (2011), 221–237, http://docplayer.net/36892561-Cybercrime-the-shifting-doctrine-of-jurisdiction.html.
23. The territoriality principle is one of several principles in public international law that apply to jurisdictional questions, this one holding that a sovereign state has the authority to prosecute criminal offences committed within its territory.
24. Approaches to cybercrime jurisdiction, *Journal of High Technology Law*, 4, 1 (2003), 3.
25. Kim Soukieh, Cybercrime – The shifting doctrine of jurisdiction, *Canberra Law Review*, 10, 1, (2011), 221–237, http://docplayer.net/36892561-Cybercrime-the-shifting-doctrine-of-jurisdiction.html.

26. One exception to this, where the trade is legal but advertising of it is illegal, is tobacco. From 1971, it became illegal to advertise cigarettes in the US on television and radio. Today, tobacco advertising is banned in some form in a number of countries.
27. For example, in 2016, UK enforcement authorities identified an advert claiming to sell carved bovine bone. An inspection of the published image revealed Schreger lines on the pieces, markings that are unique to ivory. The individual was later arrested and convicted for illegal ivory sales.
28. Figure 2 photo credits: Manis pentadactyla image by Verdammelt - CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=4145282; Manis crassicaudata image by S Megan de Wikipedia-From Wikipedia to Commons, https://commons.wikimedia.org/w/index.php?curid=3117125; Manis javanica image by Tropenmuseum, part of the National Museum of World Cultures, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8583444; Manis culionensis image by Rodine Teodoro (Philippine Postal Corporation) - [1] [2], https://commons.wikimedia.org/w/index.php?curid=49637784; Manis gigantea image by Liné1 - Picture taken with my Panasonic TZ3, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=7584748; Manis temminckii image by Masteraah, https://commons.wikimedia.org/w/index.php?curid=1525033; Manis tetradactyla image by US Fish and Wildlife Service Headquarters, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=56589245; Manis tricuspis image by Valerius Tygart, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=5613187.
29. Based on the International Union for Conservation of Nature's red list range and distribution map.
30. Personal communication, CITES Wildlife Cybercrime Working Group, April–May, 2018.
31. Personal communication with Tania McCrea-Steele, project lead, Global Wildlife Cybercrime, IFAW.
32. As one example, Regulation 01/CEMAC/UMAC/CM on the Prevention and Suppression of Money Laundering and the Financing of Terrorism and Proliferation in Central Africa (Art. 114) makes laundering of proceeds an offence (applicable to wildlife trade crimes through Arts 1(19) and 8) with a minimum fine of 10 million CFA francs and a maximum of five to 10 times the value of the property or funds involved.
33. See Guinea's Wildlife Law, which applies a minimum fine of 70 000 francs and a maximum of 150 000 francs and prison terms of three to 12 months for the unauthorized collection of eggs in a national park. Vietnam, as another example, has a substantially more complex approach, tying the fine level to the protection status of the species and the estimated value, with numerous divisions in the penalty levels.
34. See, for example, R Elvik, Cost-benefit analysis of police enforcement, Technical Research Centre of Finland, 2001, http://virtual.vtt.fi/virtual/proj6/escape/escape_wp1.pdf.
35. See, for example, D Brown, Cost-benefit analysis in criminal law, *California Law Review*, 2004.
36. Mongolia Law on Fauna, Art. 7.1, 2012.
37. Mongolia List of Rare Animals, 2012.
38. TRAFFIC Briefing, An updated review of online ivory trade in Japan, August 2017, http://www.traffic.org/home/2017/8/8/traffic-surveys-find-thousands-of-ivory-items-sold-weekly-on.html.
39. The countries reviewed are Cambodia, Cameroon, China, Congo, the Czech Republic, the Democratic Republic of Congo, France, Guinea, Indonesia, Ivory Coast, Laos, Liberia, Malaysia, Myanmar, Mongolia, Nigeria, Portugal, Rwanda, Russia, Tanzania, Uganda, UK and Vietnam.
40. US Lacey Act, 2008; EU Timber Trade Regulation, 2013; and Australia's Illegal Logging Prohibition Regulation, 2012.
41. Based on Legal Atlas database of advertising legislation compiled for the creation of a database of laws for wildlife trade.
42. Chile: New regulations in Chile restrict food advertising to children, Global Advertising Lawyers Alliance, http://www.mondaq.com/content/pr_article.asp?pr_id=15680.
43. Lorenza Ferrari Hofer, Advertising in Swiss media: Specific rules apply, Pestalozzi Attorneys At Law.
44. IFAW, Caught in the web: Wildlife trade on the internet, 2005, https://www.ifaw.org/united-states/resource-centre/caught-web.
45. People's Republic of China, Wildlife Protection Law, Art. 31, 2016.
46. Portugal Law No. 95/2017 of August 23, Regulating the purchase and sale of pets in commercial establishments and through the internet, proceeds to the sixth amendment to Decree - Law no. 276/2001, of October 17 (author's translation).
47. 'Access' is used in a legal context as a basis for determining jurisdiction based on the act of 'accessing' an internet service of some kind, as opposed to other internet-related activities, such as the hosting, registration, etc, of a site.
48. France, Article L. 412-1 of the environmental code, 2018.
49. Mongolian Law on Advertisement, Art. 14, 2002.
50. Russian Federation Federal Law amending the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation, Art. 1, amending Art. 258(1) of the Criminal Code.
51. Mongolian Law on Advertisement, Art. 14, 2002.
52. Ibid., Art. 6.5.2.
53. Ibid., Art. 6.5.8.
54. Ibid., Art. 6.2.
55. Czech Republic Act on Trade in Endangered Species, Art. 23b(1), as amended 2012.
56. UK, The Control of Trade in Endangered Species Regulations, 2018.
57. Czech Republic Act on Trade in Endangered Species, Art. 23b(1), as amended 2012.
58. J Wingard, et al, Silent Steppe: *Mongolia's Wildlife Trade Crisis, Ten Years Later.* London: Zoological Society of London, Legal Atlas, LLC and IRIM (June 2018).
59. Ibid.
60. Personal communication, CITES Wildlife Crime Working Group, April–May, 2018.
61. 12 alarming cyber security facts and stats, Cybint News, 16 March 16 2018, https://www.cybintsolutions.com/cyber-security-facts-stats/.
62. *Madagascar Loi n° 2014-006 sur la lutte contre la cybercriminalité, Art. 1.*
63. Philippines Republic Cybercrime Prevention Act of 2011, Section 6.
64. Including Madagascar, Cameroon, Ivory Coast, Malaysia, Nigeria and Oman.

65. See *Madagascar Loi n° 2014-006 sur la lutte contre la cybercriminalité, Arts. 6–15.*
66. What constitutes a 'special law' is not defined in the legislation.
67. Philippines Revised Penal Code, Art. 188, 1930 as revised 2012.
68. Ibid., Art. 196.
69. Ibid., Art. 278.
70. Ibid., Art. 188.
71. Ibid., Art. 192.
72. Ibid., Art. 196.
73. Ibid., Arts. 272–274.
74. Operation Avalanche, Tracking child porn, BBC News, 11 November, 2002, http://news.bbc.co.uk/2/hi/uk_news/2445065.stm.
75. USPS Postal Inspectors Fact Sheet, The U.S. Postal Inspection Service teams with internet crimes against children task forces in Operation Avalanche, https://postalinspectors.uspis.gov/radDocs/pubs/ar01_04.pdf.
76. Operation Avalanche, Tracking child porn, BBC News, 11 November, 2002, http://news.bbc.co.uk/2/hi/uk_news/2445065.stm; USPS Postal Inspectors Fact Sheet, The U.S. Postal Inspection Service teams with internet crimes against children task forces in Operation Avalanche, https://postalinspectors.uspis.gov/radDocs/pubs/ar01_04.pdf.
77. Code for Crown Prosecutors, Inchoate Offences Legal Guidance.
78. UK Criminal Law Act 1977, Section 1(1); Common law conspiracy applies to only two crime types – 1) conspiracy to defraud, and 2) conspiracy to corrupt public morals or outrage public decency.
79. 2006 European Data Retention Directive.
80. See German Telemedia Act, 2007 and Federal Data Protection Act, 2017.
81. Australia Telecommunications (Interception and Access) Act 1979.
82. Stored Communications Act, 18 U.S.C. § 2701 et seq., 1986.
83. Ibid., § 2703 (d).
84. UK Regulation of Investigatory Powers Act 2000.
85. Under the Australia Telecommunications (Interception and Access) Act 1979, Section 110A, access may be granted to the following: Australian Federal Police; state police forces; Australian Commission for Law Enforcement Integrity; Australian Criminal Intelligence Commission; the Immigration and Border Protection Department; Australian Securities and Investments Commission; Australian Competition and Consumer Commission; Independent Commission Against Corruption; Police Integrity Commission; Independent Broad-based Anti-corruption Commission; Crime and Corruption Commission; Independent Commissioner Against Corruption; or an authority or body for which a declaration is in force.
86. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU, September 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
87. See Privacy International, https://www.privacyinternational.org.
88. UK Regulation of Investigatory Powers Act, 2000.
89. See Privacy International, https://www.privacyinternational.org.
90. Poland, *Ustawa o zmianie ustawy o policji i innych ustaw*, 2016 Amendment.
91. Legal Atlas has not conducted an independent review of applicable data retention legislation and relies on reports that may be somewhat dated in this regard.
92. Australia's Telecommunications Information Act applies to 'relevant services', which are broadly defined as services that: 1) carry communications or enable communications to be carried by means of guided or unguided electromagnetic energy or both; 2) are operated by a carrier or carriage service provider or an ISP; and 3) are offered by a person who owns or operates infrastructure in Australia that enables the provision of any relevant service.
93. See PureVPN aided FBI to track cyberstalker by providing his logs, HackRead, October 2017, https://www.hackread.com/purevpn-aided-fbi-track-cyberstalker-providing-logs/.
94. VPN use skyrockets in Australia amid privacy concerns, CNet, 14 April, 2015https://www.cnet.com/au/news/vpn-use-increases-in-australia-amid-data-retention-and-piracy-concerns/.
95. Based on the principle of universal jurisdiction that allows any country to prosecute any person engaged in these activities.
96. B Rosenblatt, Principles of jurisdiction, https://cyber.harvard.edu/property99/domain/Betsy.html.
97. UK Financial Services Act of 1996 makes it a criminal offence to place investment advertisements in the UK unless they are issued or approved by the UK's Financial Services Authority.
98. Malaysian Computer Crimes Act, 1997 Part III, Section 9, Territorial scope of offences under this Act.
99. Nigeria Cybercrimes (Prohibition, Prevention Etc) Act, 2015, Art. 50 (d) (i) and (ii).
100. Philippines Cybercrime Prevention Act, 2012, Section 21, Jurisdiction.
101. *Zippo Manufacturing v. Zippo Dot Com*, 952 F. Supp. 1119 (W.D.Pa.1997).
102. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU, September 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
103. David A Sadoff, *Bringing International Fugitives to Justice: Extradition and its Alternatives*. Cambridge University Press, 2016, p 20.
104. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU, September 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
105. There are several examples of this type of law: the US Lacey Act, 2008; EU Timber Regulation, 2013; Australia Illegal Logging Prohibition Regulation, 2012; and the Kenya Criminal Code, 130, etc.



THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

www.globalinitiative.net

A NETWORK TO COUNTER NETWORKS