

TRANSPORT AND LOGISTICS

DISCUSSION PAPER

Challenges and good practices for transport and logistics services to prevent the use of their services for IP-infringing activities



September 2022

TRANSPORT AND LOGISTICS – DISCUSSION PAPER

Challenges and good practices for transport and logistics services to prevent the use of their services for IP-infringing activities

DISCLAIMER

The views expressed in this discussion paper do not represent the official position of the EUIPO. This paper is based on the work of the EUIPO Observatory's Expert Group on Cooperation with Intermediaries. The views expressed in this discussion paper cannot be attributed to the Expert Group as a whole or to any single contributing expert.

The Observatory welcomes any further input or comments on this discussion paper, in order to continue deepening its understanding of good practices in undermining the misuse of electronic payment services for intellectual property-infringing activities. This discussion paper may be subject to reviews or updates based on any further input from experts or new developments in the field.

ISBN 978-92-9156-325-8 DOI 10.2814/719443 TB-07-22-871-EN-N

© European Union Intellectual Property Office, 2022

Reproduction is authorised provided the source is acknowledged

Foreword

The Expert Group on Cooperation with Intermediaries was set up to further the understanding of how different intermediary services can be misused for intellectual property infringing activities, and how these misuses can be counteracted through good practices. Having looked at domain names⁽¹⁾, social media⁽²⁾ and payment services⁽³⁾, this fourth discussion paper examines transport and logistic services. It will hopefully contribute to a better understanding of:

- trends on how transport and logistic services are misused to infringe IP or support IP-infringing activities;
- the challenges raised by this misuse;
- existing and developing good practices through which they can be met;
- new technologies being developed or considered to counteract this misuse.

The initial findings of this discussion paper served as a basis for a targeted workshop organised in April 2022 by the European Commission, together with the EUIPO European Observatory on Infringements of IP rights. This workshop formed part of the stakeholder dialogue organised in the context of the EU toolbox against counterfeiting that was announced in the 2020 European Commission IP Action Plan to set out coherent, effective and coordinated action against counterfeiting, both online and offline⁽⁴⁾.

⁽¹⁾ [Domain names – Discussion paper: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities](#), (EUIPO, March 2021).

⁽²⁾ [Social Media – Discussion paper: New and existing trends in using social media for IP infringement activities and good practices to address them](#), (EUIPO, June 2021).

⁽³⁾ [Payment – Discussion paper: Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities](#), (EUIPO, November 2021).

⁽⁴⁾ Communication from the European Commission on ‘[Making the most of the EU’s innovative potential – An intellectual property action plan to support the EU’s recovery and resilience](#)’, 25 November 2020, p. 16.

Table of Contents

Foreword	3
Table of Contents	4
Executive Summary.....	6
Report Content	9
1 Introduction and background	9
1.1 Misuse of transport and logistics services for IP-infringing activities.....	9
1.2 Scope of the discussion paper.....	10
2 Mapping of the Transport and Logistics Ecosystem	11
2.1 Maritime operators.....	11
2.2 Air freight operators	13
2.3 Road operators	15
2.4 Rail operators.....	15
2.5 Parcel delivery operators	16
2.5.1 Postal service operators.....	17
2.5.2 Express service operators.....	18
2.6 Freight Forwarders	20
2.7 Logistic Centres.....	21
2.8 Custom Authorities.....	22
3 Trends and Challenges	26
3.1 Trends	27
3.1.1 Use of free trade zones	27
3.1.2 Evolution of trade routes and infrastructure development initiatives	29
3.1.3 Growth in e-commerce and the multiplications of small parcels.....	30
3.1.4 Specific tactics from IP-infringers to lower the risk of detection.....	31

3.2	Challenges	34
3.2.1	Sharing of information	34
3.2.2	Detection of IPR-infringing goods by customs	37
3.2.3	Cost of storing and destruction of IPR-infringing goods	39
4	Good Practices	41
4.1	Preventive measures	41
4.1.1	Terms and conditions and specific policies	41
4.1.2	User verification	42
4.1.3	Monitoring systems and processes	42
4.2	Strengthen cooperation	45
4.2.1	Cooperation between T&L operators and IP rights holders	45
4.2.2	Cooperation between LEAs, IP rights holders and T&L operators	46
4.2.3	Cooperation between LEAs	49
4.2.4	Cooperation between different types of intermediaries	52
4.2.5	Destruction of IPR-infringing goods	53
5	New Technical Solutions Currently Considered or Developed	54
5.1	Tracking devices	54
5.2	Blockchain based solutions	55
5.2.1	Blockchain based solutions developed by private sector	55
5.2.2	Blockchain based solutions driven by the public sector	56
6	Conclusions	57
	Annexes	58

Executive Summary

The different transport and logistics (T&L) operators form a complex ecosystem, with a number of operators taking part in large supply chains, and customs plays a central role as the public authority supervising the traffic of goods across borders. T&L operators include rail and truck operators, air freight and maritime operators, parcel delivery operators such as express service operators and postal service operators, as well as cargo owners and logistics solutions providers that organise supply and logistics, receive, store and dispatch goods (e.g. freight forwarders, distribution centres and fulfilment centres).

All these operators support international trade. However, their services are also misused by IP infringers to transport their illicit goods, with criminal groups operating across multiple jurisdictions to avoid detection and exploit the differences of the applicable national laws. In the context of this discussion paper, experts identified **existing and emerging trends and tactics to move IPR-infringing goods undetected** through the supply chain, including:

- **the use of free trade zones (FTZ)** and the reduced oversight and transparency in these zones by counterfeiters to hide the origins of IPR-infringing goods and to minimise the risks of detection;
- **the use of new trade routes and infrastructure development initiatives** by counterfeiters to find new entry points into the European Union with less control capacity.
- **the growth of e-commerce** over the last decade and the resulting multiplication of small parcels, which are used to ship IPR-infringing goods to the end consumer while lowering the potential losses in case of detentions;
- **misclassification of IPR-infringing goods** to avoid detection, including mislabelling of goods to make it difficult for T&L operators to complete risk profiling of the goods they are transporting.

Experts also identified a number of **challenges to counteract the misuse of T&L services**, including the following.

- **Sharing of information** by T&L operators with customs as part of their activities. However, T&L operators would also benefit from receiving information from customs in terms of detentions and intelligence on the latest trends and trade routes to refine their own monitoring systems. Experts also pointed to the lack of solutions to identify high risk customers that have been terminated by other T&L operators and/or other relevant intermediaries. In this context, they pointed to the need for guidance on the type of information that could be shared in line with European Union (EU) data protection and competition laws.
- **Detection of IPR-infringing goods by customs** that require physical inspection, and cannot be performed through non-intrusive imaging machines. This raises challenges for customs services that have to deal with an ever-growing number of risks. In this context, experts highlighted the importance of putting in place risk analysis systems that rely on digitised data that cannot be falsified to ensure the most effective use of customs resources.
- **Storage and destruction of IPR-infringing goods** that can be complex, lengthy and costly, and leading to disruption in supply chains, with situations where some T&L operators have to keep shipments stored in their warehouses for extended periods of time with no possibility of removing them or delivering them to their customers.

To address some of the trends and challenges faced by T&L operators, experts pointed to some good practices that exist or are being developed, as well as new technologies. These include the following.

- **Monitoring and risk profiling systems** that in addition to terms and conditions and user verification, are used by some T&L operators to detect potentially bad parties and illicit goods. These systems utilise open and undisclosed sources of information, such as denied parties lists and internal lists, combined with certain trigger words. Some operators also check consignment data, routes, or parties, to perform extensive risk profiling analysis.

- **Cooperation between T&L operators, IP rights holders and law enforcement authorities**, with initiatives at national, regional and international levels. This includes industry working groups, memorandum of understandings, joint task forces and targeted operations, as well as the development of dedicated networks with representatives from various sectors and public authorities.
- **Experts highlighted new technical solutions** as possible avenues to further counteract misuses of T&L services such as sophisticated devices tracking containers or consignments. Private blockchain-based solutions are also being developed to track and authenticate products, with the EUIPO's anti-counterfeiting blockchain infrastructure aiming at interconnecting these private solutions with law enforcement authorities to support the authentication of genuine goods throughout the supply chain.

This discussion paper will hopefully contribute to a better understanding of the very complex and innovative T&L ecosystem and of the challenges to counteract the misuse of different T&L services for IP-infringing activities. The different good practices identified will also hopefully contribute to the discussions on ways to enhance cooperation and to develop technology for all the relevant operators to jointly meet these challenges.

Report Content

1 Introduction and background

1.1 Misuse of transport and logistics services for IP-infringing activities

Along with the development of global trade, the growth of sophisticated transport and logistics (T&L) networks supported by information sharing has dramatically increased the volume of goods and information moving around the world⁽⁵⁾. Reliable and secured supply chains are central to the activities of many IP rights holders that rely on the services of T&L operators to support the distribution of their goods.

These operators play a central role in supporting international trade, by developing a broad range of solutions and innovative services to transport, store and deliver goods in the most effective way. They are constantly adapting to the changing economic and international trade landscape, to support the transport and delivery of goods, including in challenging times such as the COVID-19 crisis. These circumstances have prompted another wave of innovation to further optimise T&L services, with an unprecedented investment in tech-focused supply-chain companies⁽⁶⁾.

However, the increase in international trade has in turn resulted in a rise of illicit trade, providing a significant source of income for organised crime groups. Transport routes for drugs, firearms or IPR-infringing goods⁽⁷⁾ span across all continents through the global supply chain, with criminal groups operating across multiple jurisdictions to avoid detection and exploit the differences of the applicable national laws⁽⁸⁾.

The T&L ecosystem is made up of a diversity of operators that cover only a part of or the complete transportation of goods throughout the supply chain. This includes rail and truck operators, air freight and maritime operators (including containerships and inland waterway vessels), parcel delivery

⁽⁵⁾ [World Trade Report 2013: Factors shaping the future of the world trade](#), (WTO).

⁽⁶⁾ See [The Technology That's Helping Companies Thrive Amid the Supply-Chain Chaos](#). This investment totalled EUR 21.4 billion in the first 9 months of 2021.

⁽⁷⁾ This paper uses the term 'IPR-infringing goods' to describe tangible goods that infringe any intellectual property rights.

⁽⁸⁾ [EU Strategy to tackle Organised Crime](#) p.3 (2021, European Commission).

operators such as express service operators and postal service operators, as well as cargo owners and logistics solutions providers that organise supply and logistics, receive, store and dispatch goods (e.g. freight forwarders, distribution centres and fulfilment centres).

All these services are misused in the illegal trade of IPR-infringing goods, coming from outside the EU or circulating within the internal market.

Regarding goods detained at the EU border, data on the detentions shows that in 2020, some 27 million IP-infringing items were detained. The estimated value of these items was EUR 778 million, which corresponded to 35 % of the total value of the overall items detained at both the EU border and within the internal market. The main transport modes for bringing articles into the EU are maritime and road transport, which together represent 87 % of all shipped articles⁽⁹⁾.

- **Regarding goods detained inside the EU borders**, data on the detentions within national markets reported by 23 Member States' enforcement authorities⁽¹⁰⁾ showed that in 2020, some 46 million IP-infringing items were detained in the EU internal market by police, customs and market surveillance authorities⁽¹¹⁾. The estimated value of these items was EUR 1.3 billion, which corresponded to 65 % of the total value of the overall items detained at both the EU border and within the internal market⁽¹²⁾.

The reasons for counterfeiters to choose one means of transport or another depends on different factors, including the nature of their activities, their business models, necessity, costs, but also the risks of their illicit goods being intercepted. For example, using maritime transport and containers, allows the counterfeiters to hide IPR-infringing goods in larger consignments and avoid detection. However, using parcel delivery speeds and increases the number of deliveries and lowers the potential losses when IPR-infringing goods are detained⁽¹³⁾.

1.2 Scope of the discussion paper

⁽⁹⁾ [EU enforcement of IPR: results at the EU border and in the EU internal market 2020](#), (2021, European Commission and EUIPO), p.6-7.

⁽¹⁰⁾ *Ibid.*, p.5.

⁽¹¹⁾ *Ibid.*, p.7.

⁽¹²⁾ *Ibid.*, p.44.

⁽¹³⁾ [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), p.77.

The different T&L operators form a complex ecosystem, with a number of operators taking part in large supply chains, and customs plays a central role as the public authority that supervises the traffic of goods across borders (see section 2). The different types of transport operators use different systems to gather and share information about the goods they transport, and are governed by different rules and regulations. However, contributions from the expert group show that they face similar trends and challenges in tackling the misuse of their services for IP-infringing activities (see section 3).

This discussion paper focuses on the trends and challenges that are common to all T&L operators. It also explores broad categories of good practices that are used to counteract the entry and circulation of IPR-infringing goods (see section 4), as well as technical solutions that are being considered or under development (see section 5).

2 Mapping of the Transport and Logistics Ecosystem

With regard to transportation of goods, the terms transport and logistics tend to be used interchangeably. However, transportation is limited to moving products and materials from one place to another, including the shipment of finished products, or raw materials and product parts, as part of the manufacturing process, whereas logistics includes overseeing transportation, as well as storage of materials, production and inventory management. It can also include the packaging of products for storage and shipment.

This section aims to detail the activities, roles and responsibilities of different T&L operators, the links and relationships between them, as well as their interactions with law enforcement agencies (LEAs)⁽¹⁴⁾ and other intermediaries, throughout the supply chain.

2.1 Maritime operators

⁽¹⁴⁾For the purpose of this paper law enforcement agencies are defined as national police, customs or other authority that is authorised to detect, prevent and investigate offences and to exercise authority and coercive force.

Over 80 % of the volume of global trade in goods is carried by sea, making maritime transport the backbone of international trade. In the EU, nearly 40 % of the goods exchanged between Member States and almost 90 % of EU's imports and exports are conducted by sea⁽¹⁵⁾.

Maritime operators usually do not complete the entire supply chain, but rather play a part in it. They normally transport goods on behalf of freight forwarders (FF)⁽¹⁶⁾ or consolidators, receiving goods from them rather than the original consignor.

The normal process is the maritime operator provides an empty container at the designated premises of the shipper of the consignment⁽¹⁷⁾. The container is loaded and returned sealed, with a declaration that details its contents and provides shipping instructions, to the maritime operator's agents at the port of loading. This declaration, which includes information on the nature of the consignment and the quantity loaded in the container, flows into the **Bill of Lading (B/L)**. The B/L is a legal document that is evidence of the contract of transportation, which also serves as a receipt of the consignment taken over by the maritime operator. It allows its transfer from the shipper to the final consignee. In addition, the B/L contains information about the shipper (the person appearing as sending the shipment overseas)⁽¹⁸⁾, the consignee (the person at the destination to whom the shipment is addressed but who might be different from the ultimate receiver), the number of shipping units, classification of the goods (following HS codes)⁽¹⁹⁾, weight, description of the consignment's route, including its place of loading and place of unloading.

The B/L issued by the maritime operator is called the 'Master B/L'. In cases where transport is organised by a FF, a second set of B/L will be issued by the FF, called the 'House B/L'. The 'Master B/L' will then show the FF as shipper and one of its affiliates, agent or another FF at the port of destination that appears as the consignee⁽²⁰⁾. The 'House B/L issued by the FF might show the

⁽¹⁵⁾ See European Commission – [Mobility and transport – Maritime](#).

⁽¹⁶⁾ See section 2.6 on freight forwarders. If the large majority of maritime shipping goes through freight forwarders, major companies shipping very large volume also work directly with maritime operators. Since counterfeiters are highly unlikely to work directly with a maritime operator this section focuses on the typical case where a freight forwarder is used as an intermediary.

⁽¹⁷⁾ For the purpose of this paper a consignment is defined as goods packed together in a larger load (e.g. container) and dispatched simultaneously by the same supplier or underlying supplier to the same consignee and covered by the same transport contract.

⁽¹⁸⁾ The shipper appearing on the B/L might not be the real shipper or the original seller/producer.

⁽¹⁹⁾ See section 4.1.3.

⁽²⁰⁾ On its side, the FF issues a similar BL, called house BL, to its own customer on which the actual shipper of the cargo and its final receiver usually appear.

exporter as the shipper and the end importer as consignee but this document is never shown to the maritime operator. This leads to a situation where the maritime operator does not have information about the original shipper and the final receiver, only information about the FFs involved.

The maritime operator consolidates all the B/Ls for the consignments to be carried by one of its vessels into a cargo manifest. These manifest lists all the B/Ls and details the number of goods for each B/L. It also includes copies of all the individual B/Ls. If rules vary from one country to the other, the cargo manifest usually has to be submitted to the customs authorities at the port of origin and destination before the vessel leaves.

For maritime transports to the EU an **entry summary declaration (ENS)** has to be submitted for each cargo consignment. This cargo information has to be sent to customs authorities through a dedicated IT system⁽²¹⁾. For long haul transport, the ENS has to be submitted 24 hours before the goods are loaded at the port of origin. For short haul transport the ENS has to be submitted at least 2 hours before the arrival at the first port in the EU⁽²²⁾.

2.2 Air freight operators

According to some estimates⁽²³⁾ air freight operators transport over USD 6 trillion (EUR 5.3 trillion) worth of goods per year, accounting for approximately 35 % of world trade by value, but less than 1 % of trade by volume. In addition, they transport 328 billion letters and 7.4 billion postal parcels every year worldwide⁽²⁴⁾. The estimated annual growth rate of global air transport is about 5 %, making it a growing contributor to global trade.

There are three basic air freight models:

- **integrators or express services** who provide door-to-door services and operate their own aircrafts (see section 2.5.2),

⁽²¹⁾ More information under section 2.8.1.

⁽²²⁾ For definition of long haul and short haul transport see [\(EU\) Regulation 1875/2006](#) Article 184a.

⁽²³⁾ [IATA](#) is a trade association representing approximately 275 commercial airlines worldwide, accounting for more than 83 % of total air traffic.

⁽²⁴⁾ [Air Cargo Matters \(IATA\)](#).

- **postal operators**, who use air operator services, with air mail covered by specific regulations (see section 2.5.1), and
- **freight forwarders or consolidators**, who use the service of air freight operators from airport-to-airport in the context of their activities (see section 2.6).

These models can be mixed, with for example integrators using the services of air operators on routes for which they do not have their own air transport. Although most air cargo is flown on passenger aircrafts, aircrafts dedicated to freight (or full freighters) are used on specific high-volume routes. In some cases, FFs have their own full freighter aircrafts for specific routes. In addition, within geographical regions like Europe, air freight operators utilise a dense network of road feeder services (RFS)⁽²⁵⁾ to move ready built pallets to and from their airport hub locations. Trucks usually transport these cargos, but they are treated as air cargo with an associated flight number and manifest.

In those cases where an air freight operator transports goods on behalf of a FF, or a consolidator, the consignor usually contacts the FF and provides, inter alia, information related to itself and the consignee, the origin and the destination, the airway bill number and a description of the goods. This information is included on the **house airway bill** (HAWB) that has the value of a contract between the FF and the consignor. The FF then enlists the services of an air freight operator, who issues a **master airway bill** (MAWB) that acts as the contract between the FF and the air freight operator.

The original HAWB is always included in the MAWB. Considering that an FF might have several cargos with different HAWB's they often consolidate these into a single MAWB. As a rule, the initial data about the original consignor and final consignee, is replaced by the FFs details on the MAWB. This leads to a situation where the air freight operator does not have information about the original consignor and the final consignee in the final MAWB.

The air freight operator has to submit an **entry summary declaration** (ENS) to customs authorities when transporting goods to the EU. The ENS for long haul air transport has to be submitted at least 4 hours before arrival at the first airport in the EU. For short haul transport it has to be submitted at least by the time of the planes takeoff⁽²⁶⁾.

⁽²⁵⁾ A service offered by an air freight operator to move its carried goods to and from the aircraft and/or terminal by road service. This allows the operator to also offer its services to a city to which it does not fly aircraft.

⁽²⁶⁾ For definition of long haul and short haul transport see [\(EU\) Regulation 1875/2006](#) Article 184a.

2.3 Road operators

In 2020, road transport accounted for 19 % of EU exports and 9 % of EU imports by volume⁽²⁷⁾. According to a 2019 analysis, road is the leading mode of freight transport at intra-EU level, accounting for a 53 % share of total transport⁽²⁸⁾. Road operator's services can be used as part of a broader supply chain, or to complete the entire supply chain⁽²⁹⁾.

When they form part of a broader supply chain, transport operators usually transport goods to and from by other means of transport and on behalf of other parties such as FFs. If the road operator is used to import and/or export goods it can also act as a custom broker. For goods that are transported internationally by road a **CMR note**⁽³⁰⁾ is needed. The CMR note confirms that the road operator has received the goods and that a contract of transportation exists between the consignor and the road operator. The CMR note includes, inter alia, information on the name and address of consignor, carrier and consignee, a description and weight of the goods and instructions for customs, as well as other formalities such as dangerous goods information.

Road operators have to submit an **entry summary declaration** (ENS) to customs authorities when transporting goods to the EU. The ENS for road operators has to be submitted at least 1 hour before arrival at the first point of entry in the EU⁽³¹⁾.

2.4 Rail operators

In 2019, rail transport accounted for 17.6 % of the EU total inland freight⁽³²⁾. As with road operators, rail operators can be part of a supply chain, or complete the entire supply chain via rail networks. Rail operators are usually contracted by FFs or consolidators to complete part of the supply chain

⁽²⁷⁾ [International trade in goods by mode of transport](#). (EUROSTAT website, 11/08/2022)

⁽²⁸⁾ In [2019](#), road accounted for just over half of all tonne-kilometres performed in the EU (53.4 %). A **tonne-kilometre**, is a unit of measure of freight transport, which represents the transport of one tonne of goods (including packaging and tare weights of intermodal transport units) by a given transport mode (road, rail, air, sea, inland waterways, pipeline, etc.) over a distance of one kilometre.

⁽²⁹⁾ This section focuses on road operators carrying large consignments whilst other types of road operators, and in particular small parcel deliveries are covered in section 2.5.

⁽³⁰⁾ CMR stands for '*Convention relative au contrat de transport international de marchandises par route*'

⁽³¹⁾ See [\(EU\) Regulation 1875/2006](#) Article 184a.

⁽³²⁾ [Freight transport statistics](#) - modal split (2021, Eurostat).

on their behalf. If a rail operator is used to import and/or export goods it can also act as a custom broker.

Once the rail operator has been contacted by the consignor or an FF to transport the goods, a **rail transport document (CIM)**⁽³³⁾ is needed. This document acts as a contract between the rail operator and the consignor. The contract is concluded when the rail operator accepts the shipment, and the dispatch station's stamp (a date stamp) is placed on the CIM and the consignor/FF and the operator sign it. The CIM contains, inter alia, information on the consignor and consignee, destination, description of the goods and a detailed list of the documents that are required by customs or other administrative authorities.

A rail operator normally transports consignments from one station to another. However, in some cases they transport consignments to dedicated service centres, warehouses and/or transport hubs in the destination country that are used for subsequent dispatch and distribution.

Rail operators also have to submit an **entry summary declaration (ENS)** to customs authorities when transporting goods to the EU. The ENS for rail operators has to be submitted to customs authorities at least 2 hours before arrival at the first point of entry in the EU⁽³⁴⁾.

2.5 Parcel delivery operators

Parcel delivery operators include **postal and express services** that collectively operate 170 000 vehicles and 1 500 aircraft in 220 countries. They account for over 30 million shipments per day⁽³⁵⁾.

Parcels can be categorised using a variety of parameters⁽³⁶⁾, including weight and size, time sensitivity, mode of delivery. They usually exclude letters or other items of direct mail⁽³⁷⁾ although the increase in e-commerce has resulted in small lightweight e-commerce deliveries that frequently

⁽³³⁾ Depending on where the consignment is sent this document could also be called SMGS. A CIM is used for consignments sent to western Europe whilst a SMGS is used for consignments being sent to eastern Europe.

⁽³⁴⁾ See [\(EU\) Regulation 1875/2006](#) Article 184a.

⁽³⁵⁾ [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), p.19.

⁽³⁶⁾ In accordance with Article 2 of the [Regulation \(EU\) 2018/644 on cross-border parcel delivery services](#), parcels mean postal items that contain goods with or without commercial value, other than an item of correspondence, with a weight not exceeding 31.5 kg, and parcel delivery services means services involving the clearance, sorting, transport and distribution of parcels.

⁽³⁷⁾ [Trade in the time of parcels OECD Trade Policy Paper May 2021 n°249](#) (2021, OECD), p.10.

travel in small parcels to be treated like letters. In terms of weight, parcels are most commonly defined as goods with or without commercial value of up to 31.5 kg, but different carriers have their own definitions, with varying maximum weight and size thresholds.

2.5.1 Postal service operators

Postal service operators⁽³⁸⁾, together with express service operators, account for most of the transport of letters and parcels (postal items)⁽³⁹⁾. The growth in e-commerce counterbalances the decline in traditional mail for postal services in industrialised countries. European postal service operators delivered 7 billion parcels in 2019. In the same year, the number of letters carried by the European postal service operators exceeded 54 billion. It was estimated that in 2016, letters containing goods accounted for 80 % to 85 % of the total business to consumer (B2C) e-commerce deliveries⁽⁴⁰⁾. In 2018, goods (and documents in packages) accounted for about 58 % of the total international letters and 86 % of the weight⁽⁴¹⁾.

Postal service operators rely on other transport operators, in particular for international shipment. They also rely on other postal service operators for inward delivery to complete the postal supply chain. Each country represented in the Universal Postal Union (UPU), including all 27 EU Member States, designates the national postal service operator to deliver to any address in its territory the postal items that arrive from other countries.

When sending postal items abroad, the sender is required to include a customs declaration. The information in these declarations is the sole responsibility of the sender and cannot be verified by postal service operators whose role is limited to advising the sender to comply with the requirements of the country of origin and destination. These declarations are systematically provided in paper form, but then fed into the customs declaration system managed by UPU so that they can be exchanged electronically. Once in the system, these declarations are converted into EDI (electronic data interchange) messages, called **ITMATT**, which are sent from the postal service operator from the country of origin to the postal service operator in the destination country. These are then

⁽³⁸⁾ Postal operator - organisation licensed to provide postal services to the general public. [UPU standards glossary](#) (2014, UPU), p.17.

⁽³⁹⁾ [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), p.17.

⁽⁴⁰⁾ [User Needs in the Postal Sector](#) (2021, WIK), p.91.

⁽⁴¹⁾ [International Postal Service, Remuneration and Regulation](#) (2020, WIK), p.17.

forwarded to the customs authority in that country. These ITMATT messages have been required since 1 January 2021⁽⁴²⁾.

The postal service operators also apply a 13-character barcode (S10 barcode) on the postal item. The barcode includes a two letter designation of the type of letter or parcel being sent, a unique nine digit number identifying the letter or parcel and a two letter country code that usually allows identification of the designated postal operator⁽⁴³⁾.

Once the postal item has been collected from the sender, the postal service operator transfers it to a sorting centre for it to be sorted, screened, weighed and sent to an international transport hub. From there, the postal service operator will utilise rail, road, air or sea operators to transport the postal item to the destination country. Once the postal item has arrived in the destination country, the local postal service operator will complete the supply chain by delivering the postal item to the addressee/receiver.

2.5.2 Express service operators

Express services refer to services ensuring the delivery of a consignment in a given time, usually no more than 2 or 3 days. They play an important role in the international trade, as a means of moving consignments in a timely manner and facilitating distance selling and the speedy delivery of goods to individual consumers, although at a higher cost than traditional postal services⁽⁴⁴⁾.

Express service operators usually provide door-to-door, customs cleared, fast delivery with a track and trace service. In order to offer track and trace services they collect information electronically early in the process, before the consignment is shipped⁽⁴⁵⁾. Some of the largest express service operators control the entire supply chain using a range of their own transport modes to move consignments from the sender to the addressee. Due to the nature of their activities, express operators often use aircraft to quickly move their shipments, especially across borders.

⁽⁴²⁾ <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/nonPermanentActs/actNonPermanentRegulationsConventionFinalProtocol08-026En.pdf> (Article 17-107)

⁽⁴³⁾ [S10 Identification of postal items](#) – 13-character identifier (UPU, 2018).

⁽⁴⁴⁾ [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), p.19

⁽⁴⁵⁾ *Ibid.*, p.20.

Upon receiving a request from the sender, the express service operator will arrange to have the consignment collected and transferred to a service centre. It will then be sorted, screened, weighed and sent to a transport hub. If the express service operator acts over the entire supply chain they will also be involved in customs clearance (e.g. helping with various documents such as export declarations, help with tax declaration and payment) and final delivery to the addressee.

Rules and regulations for parcel delivery operators

Postal and express service operators are governed by a different set of rules and regulations.

Postal operators in the EU are governed by the Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service, which is mainly based on the convention and regulations of the Universal Postal Union (UPU)⁽⁴⁶⁾. The main target of the UPU is to organise and develop an international postal service, while EU rules relating to postal services seek to organise and develop postal services at an EU level, bearing in mind that EU postal services first follow UPU and secondly EU rules.

The UPU has a longstanding history of collaboration with the World Custom Organisation (WCO). Both have entered into a memorandum of understanding that identifies areas of cooperation along with specific guidelines. As a result, the UPU's convention and regulations have many references to customs issues. For example, according to Article 20 of the convention, postal operators are not liable for customs declarations and the information provided by their customers. However, they do need to take reasonable steps to inform their customers on how to comply with customs formalities and ensure that the declarations are completed in full. These declarations are then transmitted to customs according to the process described above.

Express service operators activities in the EU are governed by Regulation (EU) 2018/644 of the European Parliament and of the Council of 18 April on cross border parcel delivery services. Due

⁽⁴⁶⁾ Established in 1874, the UPU is an international institution, with 192 member countries. The UPU has an advisory, mediating and liaison role, and provides technical assistance where needed. It makes the rules for international mail exchanges and makes recommendations to stimulate growth in mail, parcel and financial services volumes and improve quality of service for customers. UPU's convention and its regulations are multilateral treaties between governments.

to the nature of their activities, express service operators normally have all the information related to a shipment in electronic form.

This allows them to run a deeper and more thorough risk analysis on the data they collect. The process of sharing this information is somewhat different from postal operators depending on what transport mode they use for their shipments. As described in section 2.5.1, postal operators send the information to the postal operator in the destination country who then share it with customs, whilst express service operators share this information with customs according to the rules for entry summary declarations.

2.6 Freight Forwarders

According to some estimates, FFs handle 65 % of cargo transported by road, 95 % of cargo transported by air and 65 % of cargo transported by ship⁽⁴⁷⁾. They play a central role in the T&L chain, as companies coordinating the shipments of consignments from a consignor to a consignee. They use different operators to best suit their clients' needs and complete the full supply chain. The FF usually also fulfils the role of custom brokers for whichever means of transport used to enter and/or exit a custom point. They can also store goods on behalf of their customers.

As the consolidator for the use of different transport modes, an FF usually has all the information about its client and the consignment, which may not be available to the different transport operators that are being used. The information about the consignment is given to the FF by their clients. As a result, they might not have the correct details of the characteristics of the products shipped, other than those communicated for transport purposes (e.g. nature of the goods, handling instructions for dangerous goods)⁽⁴⁸⁾.

⁽⁴⁷⁾ [CLECAT - the Voice of freight forwarding and logistics](#) (CLECAT).

⁽⁴⁸⁾ See [CLECAT Position Paper on EU Toolbox Against Counterfeiting](#), March 2022, p.5.

2.7 Logistic Centres

There are different types of logistics centres that are essential in most supply chains.

- **Transfer centres**, the primary role of which is cross-docking⁽⁴⁹⁾ (i.e. sorting and transshipping⁽⁵⁰⁾ of goods). These centres do not usually store any goods or have any other functions. Goods received are immediately sorted and shipped to the next destination, which requires shipping information, as well as speedy coordination between receiving and shipping operators.
- **Distribution centres** that are used to store and manage inventory, sort received goods, and have them delivered to relevant end users. Distribution centres perform a number of functions, such as order fulfilment (picking goods according to the contents of an order), distribution processing such as inspections and packaging, and shipping so that the goods arrive by the specified deadline and specifications.
- **Processing distribution centres** are logistics centres with enhanced distribution processing capacities. Compared to standard distribution centres, they perform more advanced distribution processing that requires specialised devices and equipment. These centres are equipped with product processing capacities that are similar to some factories, for example equipment to process fresh fish or meat, or assembly lines to put together different parts of a product.
- **Fulfilment centres** are the result of growth in e-commerce, which has led to fundamental changes and innovation in the T&L environment. Although in its early stage, e-commerce relied mainly on postal and/or express operators, a growing number of e-commerce operators are now relying on largescale shipping to fulfilment centres, which ensure the final distribution. Fulfilment centres are logistics centres that perform management, picking, and delivery of goods to the final consumer once the online transaction has been completed. The added value is that many of the tasks needed in the context of e-commerce transactions (e.g. receiving

⁽⁴⁹⁾ Cross-docking is a practice in logistics of unloading materials from a manufacturer or mode of transportation directly to the customer or another mode of transportation, with little or no storage in between. (13/10/2021, Wikipedia).

⁽⁵⁰⁾ Transshipment is the shipment of goods or containers to an intermediate destination, then to another destination. One possible reason for transshipment is to change the means of transport during the journey, known as transloading.

goods, receiving orders from end users, packaging, shipping, inventory management, customer data management, but also handling returns, handling complaints, and payment process) can be completed at a local logistics centre, which allows shorter delivery times.

These types of centres are normally used by online retailers or e-commerce marketplaces, with major e-commerce marketplaces developing their own fulfilment centres. These fulfilment centres are not custom warehouses⁽⁵¹⁾ so the consignors usually have to clear the goods in bulk before transferring them to the fulfilment centres.

2.8 Custom Authorities

Customs authorities play a central role in the T&L ecosystem, as the public authorities supervising the traffic of goods at the external borders and within a given country or customs union. Customs officials operate in airports, border crossings, seaports, riverports and inland customs offices⁽⁵²⁾ controlling the shipment of goods by all means of transport. In addition, customs cooperate with market surveillance authorities in certain areas to lead or cooperate on these controls. There are more than 90 000 customs officers working in more than 2 000 customs offices around the EU⁽⁵³⁾.

The role of customs keeps evolving as well as their financial functions⁽⁵⁴⁾, they provide a first line of defence against a broad range of threats such as illegal trafficking (e.g. drugs, people), dangerous goods (e.g. bombs, weapons, explosives, ammunitions), hazardous goods or IPR-infringing goods. They contribute to the fight against organised crime, smuggling, terrorism and also work towards safety of goods (e.g. compliance with food, feed and medicinal standards but also with product compliance and safety obligations). They control goods imported into the EU but also goods that are being exported, notably illegal export of waste. Protecting the environment is one of the various tasks of customs that is planned to be expanded under future environmental and social legislation that are being considered in the EU⁽⁵⁵⁾.

⁽⁵¹⁾ Where goods are held under customs bond, that is not cleared for free circulation.

⁽⁵²⁾ Including, where relevant, premises of postal and/or express courier operators.

⁽⁵³⁾ [Wise Persons Group on the reform of the EU Customs Union](#), p.11.

⁽⁵⁴⁾ Customs financial functions include the collecting of customs duties and VAT on imported goods, as well as excise duties where applicable.

⁽⁵⁵⁾ [Wise Persons Group on the reform of the EU Customs Union](#), p.12.

This growth of legislation on non-fiscal risks is a challenge for customs in that they are required to cope with a wide range of specialised risks. The role of customs also evolves to tackle market changes, and in particular the growth in e-commerce, with a number of customs authorities building capacity to deal with illegal trade online, including the online sale of IPR-infringing goods.

In 2020, the EU customs ‘handled the import, export or transit of over 1 069 million articles’ and collected EUR 24.8 billion in customs duties⁽⁵⁶⁾. As for counterfeiting, goods with a value of almost EUR 2 billion were detained in the EU’s internal market and at external borders. At EU’s external borders, customs authorities detained fake products with a retail value of EUR 778 million⁽⁵⁷⁾.

One of customs’ main objectives is to facilitate legitimate trade. The World Trade Organisation (WTO) Trade Facilitation agreement that came into force in 2017⁽⁵⁸⁾ provides for simple and harmonised customs procedures to support the efficient transport of goods between countries, and the growth of international trade. ‘It calls for members to provide pre-arrival information on exports to destination countries in electronic format and for importing countries to develop the capacity for processing such information (...). The agreement also calls for members to adopt or maintain a risk management system (...). Members are expected to concentrate customs control (...), on high-risk consignments and expedite the release of low-risk consignments, but at the same time, are free to select, on a random basis, consignments for such controls as part of its risk management. Finally, the agreement calls on countries to develop or maintain procedures allowing for the expedited release of at least those goods entered through air cargo facilities, to persons who apply for such treatment (...)’⁽⁵⁹⁾.

The WTO agreement reflects on a broader modernisation process of customs procedure and control methods that has been ongoing in a number of countries for many years. The aim is to balance the need to deal with a greater diversity of threats (e.g. terrorism), with the facilitation of legitimate trade. The key components of this modernisation process are digitisation, the development of advanced information and risk assessment systems, as well as strengthen cooperation between customs administrations, but also with other governments agencies and businesses.

⁽⁵⁶⁾ See European Commission: [EU Customs Union – unique in the world, Custom Union in numbers 2020](#).

⁽⁵⁷⁾ See European Commission: [Taxation and Customs Union – Intellectual Property Rights – Fact and figures](#).

⁽⁵⁸⁾ [WTO Agreement on Trade Facilitation](#).

⁽⁵⁹⁾ [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), p.22.

Advanced information and the EU Import Control System

Following the September 2001 terrorist attacks in the United States, the World Customs Organisation (WCO) adopted the SAFE Framework of Standards (SAFE)⁽⁶⁰⁾. It introduced security measures for supply chains, including the requirement of advanced cargo data, security risk assessment, as well as an industry partnership programme, the 'Authorised Economic Operator' or AEO.

In the EU, customs regulations were amended to require certain data to be sent to the EU customs office of first entry, before the goods entered the territory and in most cases, even before leaving the country of export. The **import control system (ICS)** came into force at the end of 2010, as the electronic security declaration management system for the importation of goods into the EU.

Following the Yemen incident in October 2010, further measures were put in place to improve air cargo security. The EU introduced significant changes in the process for goods entering in or transiting through the EU, with regard to the risk analysis for security and safety purposes. The implementation of this new customs pre-arrival security and safety measures was underpinned by a large-scale advance cargo information system – **import control system 2 (ICS2)**.

ICS2 is a part of the EU-wide automated import system, created to collect data about all goods entering the EU prior to their arrival. Carriers – or their representatives – have to declare safety and security data to ICS2, through the **entry summary declaration (ENS)** lodged at the first point of entry (first airport, port, border crossing) into the customs territory of the EU, even if the final destination of the cargo is outside the EU. The main purpose of the ENS is to carry out risk analysis related to public health and safety, which allows customs and operators to take action before the goods are loaded at the point of departure or at its first entry into the EU.

EU Member States are responsible for performing risk analysis based on the ENS information and agreed EU risk profiles. Depending on the risk level, they are also responsible for passing on the information of their analysis to the subsequent customs offices for the cargo's journey.

⁽⁶⁰⁾ [SAFE framework of standards.](#)

The ICS2 is not a substitute for the normal custom import declarations, its implementation is through successive phases, according to specific types of transport services. It already applies to air express and postal air pre-loading and will apply to air cargo in 2023, and to maritime, road and rail in 2024.

In the context of their activities, customs interact with all types of T&L operators. Although the process varies for different countries and means of transport, it is usually the destination customs office or first entry of the goods that receives pre-arrival information from the carrier, and carries out security and safety risk analysis. ‘Upon arrival of the means of transport, the carrier must inform the customs office of first entry of its arrival. (...) From the time of entry, the goods are subject to customs supervision and customs controls. (...) If a risk is identified, the Customs Authority will take the necessary measures, including confiscating, sale or destruction of the goods’⁽⁶¹⁾.

Risk assessment from customs to target controls or verifications

In the context of their activities, EU customs authorities carry out security and safety risk analysis based on pre-arrival information from the carriers. The ICS2 programme is a central initiative in establishing an integrated EU approach to reinforce such risk management under the Customs Risk Management Framework (CRMF)⁽⁶²⁾. Within this framework the European Commission has adopted a set of criteria to be applied in the Member States’ risk analysis systems in order to continuously screen electronic advance cargo information for security and safety purposes. To assess the risks and respond appropriately, a set of criteria for security and safety purposes were developed. The criteria are included in the Member States’ risk analysis systems and are used to control consignments crossing the EU border 365 days a year⁽⁶³⁾.

The common customs risk management system (CRMS) is designed to provide a fast and easy-to-use mechanism to exchange risk-related information directly amongst operational officials and risk analysis centres in all Member States. It facilitates EU-wide customs intervention for the highest risks at the external frontier and inland and is thus an integral element in the development

⁽⁶¹⁾ See DG TAXUD ‘[Entry of Goods and Temporary Storage](#)’, p.3-4.

⁽⁶²⁾ See https://ec.europa.eu/taxation_customs/asures-customs-risk-management-framework_en and https://ec.europa.eu/taxation_customs/customs-risk-management-framework-crmf_en.

⁽⁶³⁾ Information included in Applications for Action (AFAs) are taken into consideration when doing risk assessments.

of a European Union risk management framework. It is a form (risk information form, called RIF) to be completed on-line and instantly made available to all customs offices connected. The RIF is an effective means of ensuring that a consistent level of customs control is applied at the external frontier of the European Union in relation to identified new risks. There are ongoing initiatives to improve this system, for example by carrying out risk assessments on a European level, with the possibility for Member States to include additional criteria at national level.

With regard to IPR-infringing goods, customs also interact with relevant IP rights holders, that are contacted to decide if goods detained are effectively infringing their rights and if they should be destroyed (see section 3.2.3).

In the EU, the collaboration between IP rights holders and customs is regulated under Regulation (EU) 608/2013⁽⁶⁴⁾ and detentions are based on a request from IP rights holders to customs to act and enforce their IP rights using a standard application for action (AFA)⁽⁶⁵⁾. Applications for action can be requested on a national ('National application') or on a European Union basis ('Union application') and are valid for a maximum of 1 year at a time (see also section 4.2.2). EU customs also have the power to act ex officio if they suspect an IPR infringement. In these procedures, customs have to identify the rights holder who must submit a national application within 4 working days for customs to be able to continue the detention or suspension or the release of the goods⁽⁶⁶⁾.

3 Trends and Challenges

Studies⁽⁶⁷⁾ have shown the capacity of IP infringers to quickly adapt to the evolution of the T&L landscape and law enforcement practices to minimise the risk of their shipments being intercepted. Experts identified a number of relevant trends in that respect (section 3.1), as well as challenges to counteract the misuse of T&L services for IP-infringing activities (section 3.2).

⁽⁶⁴⁾ [Regulation \(EU\) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation \(EC\) No 1383/2003.](#)

⁽⁶⁵⁾ [Regulation \(EU\) 1352/2013 establishing the forms provided for in Regulation 608/2013 concerning customs enforcement of intellectual property rights.](#)

⁽⁶⁶⁾ Article 5(3) and Article 18 of (EU) [Regulation 608/2013](#).

⁽⁶⁷⁾ See for example [Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends](#) (2018, OECD & EUIPO), [Misuse of Containerised Maritime Shipping in the Global Trade of Counterfeits](#), (2021, OECD/EUIPO) and [Intellectual Property Crime Threat Assessment 2022](#) (2022, EUROPOL/EUIPO).

3.1 Trends

Experts have identified a number of tactics from IP infringers to move their illicit goods undetected throughout the supply chain.

3.1.1 Use of free trade zones

Free Trade Zones (FTZs)⁽⁶⁸⁾ are designed to attract new and foreign businesses by eliminating tariffs, quotas and other taxes that normally apply in a given country, as well as minimising bureaucratic requirements, including certain customs procedures and disclosure requirements. These are designated areas that in most cases lie outside the customs jurisdiction of the country in question. The FTZ is most often connected to a transport infrastructure (e.g. a port or an airport) and range in size from single warehouses to massive complexes comprising thousands of businesses. Once in an FTZ, goods can be moved for several operations, such as storage, assembly, manufacturing and processing⁽⁶⁹⁾.

There has been a dramatic growth in the number of FTZs over the past decades, from 79 FTZs in 1975, to over 5 000 today, with an additional 500 planned in the next few years⁽⁷⁰⁾.

Although the FTZs bring economic benefits to the countries establishing them, they can also be misused by criminal groups for illicit trade, looking to benefit from reduced oversight and transparency in the zones⁽⁷¹⁾.

Experts pointed to the trend of IP infringers using multiple FTZs in their operations. Once the IPR-infringing goods are moved into an FTZ the counterfeiters may change the goods attributes such as assembling, re-packaging and re-labelling, before importing them into the national territory of the

⁽⁶⁸⁾ OECD defines 'Free Trade Zone' as an area designated by a country or jurisdiction, where goods that enter this area are not subject, or are subject to lower import or export duties than those that would apply if these goods were declared for release for free circulation, at the moment when they enter it. Facilities used for temporary storage or for the customs warehousing procedure are not deemed to be free trade zones. See [Recommendation of the Council on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones](#) (2019, OECD), Article 1, p.6.

⁽⁶⁹⁾ [Controlling the zone: balancing facilitation and control to combat illicit trade in the world's free trade zones](#) (2020, BASCAP), p.6.

⁽⁷⁰⁾ Ibid. p.7.

⁽⁷¹⁾ [Trade in Counterfeit Goods and Free Trade Zones](#) (2018, OECD & EUIPO), p.14.

hosting state⁽⁷²⁾. In some instances, different steps (e.g. assembling and packaging) can take part in different FTZs to reduce the risks of detection and establishing the origin of the IPR-infringing goods.

Given the growth in FTZs and their use in the context of illicit trade, including IPR-infringing goods, some experts have voiced the importance that standards, overseeing and regulations keep pace with such development. For example, the TRIPS agreement⁽⁷³⁾ does not oblige members to make border measures available with respect to transhipped goods. In addition, some governments and customs authorities believe that they might not have jurisdiction to exercise control in FTZs⁽⁷⁴⁾.

However, some standards and measurements have been developed to mitigate the risks for FTZs to be used for illegal trade in general and the trade in IPR-infringing goods in particular. This is the case of the OECD recommendations that aim to enhance and ensure transparency in FTZs as part of the broader effort to counter illicit trade, and includes a 'Code of Conduct for Clean Free Trade Zones'⁽⁷⁵⁾. Among different measures the code of conduct makes clear that clean FTZs are those that '(e)nsure that economic operators active in the FTZ maintain detailed digital records of all shipments of goods entering and leaving the zone, as well as all goods and services produced within it (...) and access to these records upon request of the competent authorities in the jurisdiction where the zone is established.' Compliance with all the provisions of the code of conduct will be assessed and monitored.

This is also the case of the WCO 'Practical Guidance on Free Zones'⁽⁷⁶⁾ that aims to help customs authorities enhance the procedures and controls to be globally applied in FTZs, while supporting their development and competitiveness.

⁽⁷²⁾ See European Commission report on ['the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities'](#), (2019, European Commission), p.5. See also [Controlling the zone: balancing facilitation and control to combat illicit trade in the world's free trade zones](#) (2020, BASCAP), p.7.

⁽⁷³⁾ [TRIPS Agreement](#).

⁽⁷⁴⁾ [Controlling the zone: balancing facilitation and control to combat illicit trade in the world's free trade zones](#) (2020, BASCAP), 2020, p.8.

⁽⁷⁵⁾ [Recommendation of the Council on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones](#) (2019, OECD).

⁽⁷⁶⁾ [World Customs Organization, Practical Guidance on Free Trade Zones](#), December 2020.

3.1.2 Evolution of trade routes and infrastructure development initiatives

Ongoing and planned infrastructure developments in the EU could significantly change trade routes for shipments, offering new avenues for illicit trade and calling for adapting control capacities.

The Chinese Belt and Road Initiative (BRI) is of particular relevance in this context. This global initiative aims to strengthen container trade connections between China and the European Union through increased connectivity between a number of countries⁽⁷⁷⁾. The initiative is a network of interconnected land transport corridors, as well as new maritime routes (see Annex 1).

Several economic studies highlight that BRI-related enhancement in infrastructure in south east Europe are likely to result in significant growth in cargo transhipped in Mediterranean ports⁽⁷⁸⁾, which play a central role in the BRI network as a ‘hub-of-hubs’⁽⁷⁹⁾. Experts mentioned that although the development of the BRI is a positive development for legitimate trade, it also raises concerns as a large share of IPR-infringing goods imported to the European Union come from China⁽⁸⁰⁾.

In this context, one of the identified risks is a shift in port operators’ incentives towards a reduction of transport time in lieu of a thorough control of shipments. This shift would likely counteract counterfeit detection and might result in substantial growth of fake products entering the EU, for example, in container ships⁽⁸¹⁾. After completion of investments in the infrastructure in south east Europe, and in line with findings of OECD, ports in the Mediterranean region could become more intensely targeted by criminal networks in the context of smuggling fake products to the EU.

The BRI also includes the development of new projects and infrastructure to develop freight trains that have significantly reduced the time and cost it takes to transport goods from China to the EU. Experts explained that a number of cities on the eastern European border were becoming major

⁽⁷⁷⁾ [The Belt and Road Initiative: Impacts on Global Maritime Trade Flows Discussion Paper](#), International Transport Forum 2020, OECD/ITF), p.4.

⁽⁷⁸⁾ [Assessing the impact of the maritime silk road’: Journal of Ocean Engineering and Science](#), Volume 2, Issue 3 September 2017 (Schinas O. and A. Graf von Westarp), p.186-195.

⁽⁷⁹⁾ [The Belt and Road Initiative: Impacts on Global Maritime Trade Flows Discussion Paper](#), International Transport Forum 2020, OECD/ITF), p.4.

⁽⁸⁰⁾ [EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020](#), (2021, European Commission & EUIPO), p.25: ‘China is the main country of provenance (50 %) from where suspected IPR-infringing goods arrived when they were detained, and where those goods were subsequently not released. (...) With regard to countries of provenance in relation to value, China is at the top of the list (...).’

⁽⁸¹⁾ [Misuse of Containerised Maritime Shipping in the Global Trade of Counterfeits](#), (2021, OECD/EUIPO), p.66.

transit points for goods entering the EU, and that there may be need to carefully monitor the evolution of these new trade routes and their use for illegal trade, including for IPR-infringing goods and to adapt customs control capacity if needed.

Experts also highlighted the intentions to create new FTZs along the BRI, which could drive trade in IPR-infringing goods in economies with weak governance, high corruption levels and a lack of intellectual property rights⁽⁸²⁾.

3.1.3 Growth in e-commerce and the multiplications of small parcels

The business of selling goods to consumers online has increased significantly in recent years. Online sales increased 25.7 %⁽⁸³⁾ in 2020 with the COVID-19 pandemic accentuating the already initiated growth⁽⁸⁴⁾. Experts indicated that the increase of e-commerce and the COVID-19 pandemic have affected the way goods are shipped, with air transport being increasingly used to meet consumer's expectation of a quick delivery.

This has also resulted in a larger misuse of services supporting e-commerce for illicit trade⁽⁸⁵⁾. For the counterfeiters, small parcels – which often travel in the mail – have become a popular means of shipping, as they lower the potential losses in case of detentions. While IPR-infringing goods shipped by container ships still dominate in terms of value, shipping of fake products by small parcels is growing and dominates in terms of the number of detentions⁽⁸⁶⁾. Between 2017 and 2019, 77 % of global detentions involved items shipped by post or express services⁽⁸⁷⁾.

The use of postal services provides counterfeiters with a reliable and cost effective service. Since 15 March 2021, parcels sent by post are subject to security and safety pre-arrival requirements and, since 1 July 2021, they must be declared at import by an electronic customs declaration (see section 2.5.1). This enables customs authorities to carry out automated risk analysis on the goods and to check their compliance with the customs and value added tax (VAT) rules and other import prohibitions and restrictions, including the import of IPR-infringing goods.

⁽⁸²⁾ Ibid.

⁽⁸³⁾ [E-commerce challenges in illicit trade in fakes: Governance frameworks and best practices](#) (2021, OECD).

⁽⁸⁴⁾ [EUIPO and OECD on misuse of E-Commerce for Trade in Counterfeits](#) (2021, OECD/EUIPO), p.8.

⁽⁸⁵⁾ Ibid., p.17.

⁽⁸⁶⁾ [EUIPO and OECD on misuse of E-Commerce for Trade in Counterfeits](#) (2021, OECD/EUIPO), p.73.

⁽⁸⁷⁾ [Global Trade in fakes: a Worrying Threat](#) (2021, OECD/EUIPO), p.23.

The rise in e-commerce has increased the demand for freight forwarding services and even resulted in the development of new operators. Some of the largest e-commerce marketplaces are setting up hubs and fulfilment centres around the world, including the EU, to be able to deliver products of their sellers. These companies are also moving into the logistics sector where they now have their own fleet of cargo planes, trucks and express services.

The growth of e-commerce is also leading to the development of new services in the T&L landscape, with experts pointing to new **parcel forwarding services**. These services allow their users to buy products from e-commerce services that do not deliver to their countries, by making it possible to have their online purchases delivered to one of their local facilities. When receiving the delivery, the parcel forwarding service will forward it to the user, or have it stored to be grouped with other parcels in a single consignment to lower the transport costs.

Those kinds of services are usually used for perfectly legitimate purposes. However, some experts highlighted that they can also be misused to disguise the actual origin/sender of a parcel. In addition, since the user is in charge of completing the necessary information for customs when requesting the forwarding of the parcel, some experts pointed out that the information provided may not correspond to the actual content of the parcel or of the grouped parcels.

3.1.4 Specific tactics from IP-infringers to lower the risk of detection

Experts have highlighted tactics used by IP infringers to lower or avoid risk of detection. A number of studies⁽⁸⁸⁾ show that the shipment of small parcels has increased in the last couple of years. Furthermore, these studies also state that whilst small parcels dominate in terms of detentions⁽⁸⁹⁾, goods shipped with containers still represent the highest number in terms of value. Some experts have pointed out that the growth in small parcels and as a result, detentions of the same, has **given rise to a modus operandi of the counterfeiters in that they send smaller packages (already packed and ready for distribution) in containers**. Once the containers reach their destination

⁽⁸⁸⁾For example, [Misuse of Small Parcels for Trade in Counterfeit Goods](#) (2018, EUIPO/OECD), p.77 and [Intellectual Property Crime Threat Assessment 2022](#) (2022, EUROPOL/EUIPO), p.8.

⁽⁸⁹⁾[Global Trade in Fakes A Worrying Threat](#) (EUIPO/OECD 2021), p.23 and [EU enforcement of IPR: results at the EU border and in the EU internal market 2020](#), (2021, European Commission and EUIPO), p.7.

country or, in some cases, the country within the same continent (such as Europe), each parcel will be shipped to the final customer or distributor.

Furthermore, some experts also pointed to the fact that **counterfeiters are deliberately targeting certain EU entry points**. The reasons for this vary but normally they target small ports that have limited customs resources or clearance procedures. This is particularly true for ports that have customs clearance at the destination port under the external union transit procedure (T1 procedure)⁽⁹⁰⁾. The procedure allows customs clearance to be postponed to the destination port rather than at the point of entry in the EU. The counterfeiters deliberately choose this method to target small inland ports where they do not have the same resources as the larger ports. External factors also affect the choice of ports because they temporarily affect customs resources for a limited time, such as the COVID-19 pandemic⁽⁹¹⁾.

Another method highlighted by the experts, is where counterfeiters are **sending branded logos, labels, tags, packaging and unbranded goods (e.g. clothes) separately to avoid detection** by customs. This has also been confirmed in a recent study that shows that labels, tags, etc. have been detained in increasing numbers⁽⁹²⁾. In addition, if these goods are detained it results in a lesser fine considering that it is calculated on the basis of the value of the original product. The counterfeiters then assemble the final product within the destination country⁽⁹³⁾.

Another way, as pointed out by the experts, for counterfeiters to **avoid custom inspection is to misclassify⁽⁹⁴⁾ or undervalue the goods shipped**. One reason for this was to come under the rules that stated that goods coming from outside the EU and had a value of less than EUR 22 were exempt from VAT. However, since 1 July 2021, this exemption has been removed, which means that all commercial goods imported into the EU from a third country or third territory are subject to VAT irrespective of their value and the taxes are to be paid by the seller. This system, IOSS⁽⁹⁵⁾, was created to facilitate and simplify the declaration and payment of VAT for goods sold from a distance by sellers from either the EU or from a non-EU country or territory. The sellers do not have to be

⁽⁹⁰⁾ [Transit manual](#), p.42.

⁽⁹¹⁾ [Global Trade in Fakes A Worrying Threat](#) (EUIPO/OECD 2021), p.60.

⁽⁹²⁾ [EU enforcement of intellectual property rights: results at the EU border and in the EU internal market 2020](#), (EUIPO/DG TAXUD 2021), p.38.

⁽⁹³⁾ According to experts another way is to declare the goods under another brand to avoid scrutiny from customs.

⁽⁹⁴⁾ Meaning that the counterfeiters use another description for the goods than what is actually shipped or change other information that is relevant for risk profiling such as sender name, point of origin.

⁽⁹⁵⁾ [Import One Stop Shop](#).

registered in the system, however, it does not remove the responsibility to pay VAT and/or taxes. This obligation is then transferred to the buyer instead. This system could potentially lower the incentive for both seller and buyer to purchase illicit goods.

The practice of misclassifying goods could have other serious effects than just avoiding customs inspections. Some experts mentioned that it is sometimes difficult for air freight operators to get accurate information about the goods they are transporting. Experts explained that counterfeiters mislabel their goods and forge shipment manifests and various certificates, for example the certificate of origin⁽⁹⁶⁾. The use of different operators and trade routes might also affect the accuracy of the documentation that accompanies the goods transported by air freight.

This is a particularly acute challenge, as reliable information is needed for air freight operators to do a complete risk profiling before they load and transport the shipments on their aircraft. In certain cases, this information is not provided or at least not provided completely and in a correct and timely manner⁽⁹⁷⁾. In addition, they point to a lack of information about the end use of the goods for air freight operators to properly determine compliance with, for example, trade sanctions and brand protection.

One reason for the above is the **lack of digitisation** within the transport and logistics ecosystem. There are several initiatives within the transport industry to digitalise all the documentation needed to transport goods from their origin to their destination (see also regulatory initiative under section 3.2.1). Within the operators' own business, it seems like most of the information they collect (details of consigner, consignee, information about the consignment, etc.) are already digitalised, at least for the larger operators in the industry. However, they normally use their own systems and nothing is centralised into one large system. This means that one operator collects information that will need to be transferred somehow to the next operator if they do not control the entire supply chain, as with express services.

For documentation that is not digital it is easier for counterfeiters to change, manipulate and hide real information about the product and its origin, especially if they are using different operators and routes between the origin and destination. If this information was digitalised it would make these

⁽⁹⁶⁾ [Certificate of Origin](#).

⁽⁹⁷⁾ In addition, some experts pointed out that the practise of mislabelling can have serious effects on the environment due to the nature of the goods and whether they are stored properly (e.g. crop protection products).

alterations more difficult, while facilitating automated data analysis to identify suspicious activities and patterns. As mentioned, some operators control the entire supply chain and are therefore able to keep all their information electronic. However, within some sectors (e.g. maritime) it is still possible for people and companies to use paper bill of lading, which are easily manipulated.

This poor quality of data, and in some instances lack of data, is also pointed out by the Wise Persons Group on the reform of the EU Customs Union in their latest report. They state that the:

poor availability and quality of the data submitted to customs, the lack of a common data warehouse, and the low level of data sharing across customs administrations leads to fragmentation and makes it extremely difficult to properly manage risks through data analytics at both national and EU level. This is a major inhibitor in a digital world where any transformation is highly dependent on the quality and availability of data.⁽⁹⁸⁾

Furthermore, some experts pointed to the challenge of identifying customers shipping IPR-infringing goods across different express service operators. Express service operators terminate the contract with customers that are in breach of the terms of their contract by, for example, shipping IPR-infringing goods. However, experts highlighted that it is common for terminated customers to quickly **swap networks** and move to another express service operator to continue their illegal activities.

3.2 Challenges

Experts pointed to a number of challenges to counteract the misuse of T&L services by IP infringers and reinforcing some of the trends identified.

3.2.1 Sharing of information

As part of their activities, T&L operators share information with public authorities, and in particular customs (see section 2). Although this information can be used by customs to feed into risk profiling systems supporting targeted inspections, experts considered that this and furthering the exchange of information from law enforcement authorities, as well as in between T&L operators or other types of intermediaries, was a major challenge and opportunity. In addition, and as pointed out by the Wise

⁽⁹⁸⁾ [Wise Persons Group on the reform of the EU Customs Union](#), p.22.

Persons Group in their latest report, this information (e.g. information about consignor, consignee, transport operator, financial information) is ‘not connected into data points and the intelligence that can be generated is limited. As a result, customs currently spend too much time and resources checking the correctness of “declarative” information and is often unable to confirm the correctness of the data and is certainly incapable of controlling all suspicious cases’⁽⁹⁹⁾.

- **Sharing of information with law enforcement authorities:** as part of their efforts to limit the misuse of their services some T&L operators have developed monitoring systems, running risk analysis on the data they have on shippers and consignments to detect potentially bad parties and illicit goods (see section 4.1.3). In this context, experts explained that these monitoring processes could be further improved if T&L operators had access to the following.
 - **Information on consignments detained and the reasons for detention:** some monitoring systems are based on the detection of signals and patterns that are used by IP infringers in the context of their activities. These signals and patterns are best identified and updated through the analysis of the data for consignment that were effectively used for illicit goods. In this context, some experts explained that getting information from law enforcement authorities on detained consignments and the reasons for detention should contribute to constantly refining monitoring and risk assessment models.
 - **Intelligence on the latest trends and trade routes** with regard to the production and transport of illicit goods in general, and IPR-infringing goods in particular. One expert explained that if transport operators rely on open source intelligence (OSINT) in the context of their monitoring process, they would additionally benefit from any intelligence shared by law enforcement authorities or governmental agencies.
- **Sharing of information with other T&L operators or other types of intermediaries:** some experts highlighted the lack of solutions to identify high risk customers that have been terminated by other operators and limit network swapping, in particular with regard to the

⁽⁹⁹⁾ [Wise Persons Group on the reform of the EU Customs Union](#), p.23.

misuse of express operator services⁽¹⁰⁰⁾. They also explained that in the context of the online sale of IP-infringing goods, services from different types of intermediaries, such as express operators, payment processors and e-commerce marketplaces, are typically misused. In this context, they pointed to the Electronic Commerce Working Group formed by the US government that includes e-commerce marketplaces, express operators and payment processors, to explore ways to enhance data sharing among different operators and other parties, and ultimately with LEAs (see section 4.2.4). In order to support the sharing of information with other T&L operators, or other types of intermediaries, experts pointed to the need for guidance that would detail what information could be shared in line with EU data protection and competition laws.

- **Enhanced use of information already shared with different public bodies:** some experts explained that the data shared with customs, are in some instances too limited or of insufficient quality to effectively support customs enforcement. They considered that this could be tackled by enhancing the use of information already shared by different intermediaries in the supply chain with different public bodies. In this context, they pointed to the forthcoming revision of the European Union customs legislation that will aim at ‘improving the controls of e-commerce to the benefits of (...) citizens (protection against non-compliant products)’ and ‘(...) will foresee a better allocation of tasks and improved exchange of information between customs and sectorial authorities so that customs authorities and the Commission are in a position to use more electronic customs data to improve the efficiency of their controls of financial and non-financial risks, thereby reducing the burden on economic operators’⁽¹⁰¹⁾. Some experts considered that with regard to e-commerce consignments, these revisions were an opportunity to reinforce cooperation between customs and tax authorities and cooperation with other authorities and identify an innovative customs approach for the identification of non-fiscal risks, including non-compliant and IP-infringing goods.

⁽¹⁰⁰⁾ These solutions exist in the payment sector with regard to credit card networks that have developed Terminated Merchants Files. See Discussion paper on Payment: [Challenges and good practices for electronic payment services to prevent the use of their services for IP-infringing activities](#), November 2021, p.26-27.

⁽¹⁰¹⁾ See: [Annexes to the Communication from the Commission on Commission work programme 2022, Making Europe Stronger Together, October 2021](#), p.9.

EU initiatives to enhance data sharing in freight transport and logistics

There are a number of new regulations aimed at enhancing the exchange of data between T&L operators and LEAs.

The **EU regulation establishing a European maritime single window environment**⁽¹⁰²⁾ includes a set of measures to achieve harmonisation and simplification in maritime reporting. It creates a single-entry point per Member State and will minimise duplication of reporting requests for static data by appropriate data re-use mechanisms. A cornerstone of the new regulation is the harmonisation of data definitions and formats and measures to improve data flows. The new environment will also allow maritime operators to report to customs through the same interface. The regulation will be fully applicable by 15 August 2025.

EU regulation on electronic freight transport information (eFTI)⁽¹⁰³⁾. The eFTI regulation entered into force in August 2020, and is going through preparatory work for technical implementation rules. The result will be a uniform EU framework for electronic information exchanges between the economic operators and the Member States authorities on cargo transport in the European Union by road, rail, inland waterways and air. It will allow the economic operators to record the cargo-related information only once and share it electronically with the authorities, or with their business partners, anytime, anywhere in the EU. The eFTI regulation will start in August 2024, with the obligation for authorities to accept the electronic information starting in August 2025.

3.2.2 Detection of IPR-infringing goods by customs

Customs have to deal with an ever-growing number of specialised risks (see section 2.8). With regard to the detection of IPR-infringing goods, experts explained that customs detection capacities are lowered by the fact that these goods cannot be detected through non-intrusive imaging machines, but only through physical inspections. Since “the external features of counterfeit goods barely differ from their legitimate counterparts, scanning of containers is not as effective in detecting

⁽¹⁰²⁾ [Regulation \(EU\) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment.](#)

⁽¹⁰³⁾ [Regulation \(EU\) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information.](#)

counterfeit goods as other types of illegal goods (...)’⁽¹⁰⁴⁾. Physical searches are resource intensive and require specially trained customs officials, as well as dedicated facilities. The rapid growth of e-commerce has also resulted in additional constraints for customs in that they have:

an exponential and unmanageable flow of millions of small individual consignments to be controlled and checked for fiscal and non-fiscal requirements. (...) Evidence also suggests that the probability that small consignments will contain non-compliant or dangerous goods is very high. It is not only that checking each parcel is impossible; it is that even checking all those that are identified as presenting a risk is unmanageable⁽¹⁰⁵⁾.

In addition, in many instances customs officials need the active involvement of IP rights holders to confirm that the goods detained are effectively infringing their IP rights.

If there is no data on the percentage of shipments entering the EU that are physically controlled by customs, for maritime transport ‘interviews with enforcement officials point that on average less than 2 % of containers incoming to the EU are inspected. Importantly, raising of this share seems virtually impossible. A physical inspection of all containers that arrive on a single ship would require tens of thousands of customs inspectors at port’⁽¹⁰⁶⁾.

In this context, some experts pointed to the importance of risk analysis systems relying on shipment data that cannot be falsified to ensure the most effective use of available customs resources to lead physical searches for IPR-infringing goods.

They also pointed to the European Multidisciplinary Platform Against Criminal Threat (EMPACT) for 2022-2025 that sets the EU priorities for the fight against serious and organised crime. The operational action ‘IP crime, counterfeiting of goods and currencies’ aims to ‘combat and disrupt criminal networks and criminal individual entrepreneurs involved in IP crime and in the production, sale or distribution (physical and online) of counterfeit goods or currencies, with a specific focus on goods harmful to consumers’ health and safety, to the environment and to the EU economy’⁽¹⁰⁷⁾. Experts considered that it was an opportunity to strengthen the cooperation between EU LEAs and

⁽¹⁰⁴⁾ [Misuse of Containerised Maritime Shipping in the Global Trade of Counterfeits](#) (2021, OECD & EUIPO), p.22.

⁽¹⁰⁵⁾ [Wise Persons Group on the reform of the EU Customs Union](#), p.12.

⁽¹⁰⁶⁾ [Misuse of Containerised Maritime Shipping in the Global Trade of Counterfeits](#) (2021, OECD & EUIPO), p.22.

⁽¹⁰⁷⁾ See [Europol, EU Policy Cycle - EMPACT](#).

private operators and parties in the detection and confirmation of the IP-infringing nature of counterfeit goods entering the EU.

3.2.3 Cost of storing and destruction of IPR-infringing goods

European Union Regulation 608/2013 concerning customs enforcement of intellectual property rights⁽¹⁰⁸⁾ governs the customs role and obligations to enforce IPRs at EU borders. It empowers EU customs to detain goods, which are suspected of infringing different types of IPR. Customs can detain goods *ex officio* or on the basis of an application for action (AFA) submitted by rights holders (section 2.8).

Under the **standard procedure**, when detaining goods suspected of IPR infringement, customs have to notify the relevant IP rights holder, as well as the declarant or holder of the goods⁽¹⁰⁹⁾ and provide information on the actual or estimated quantity and the actual or presumed nature of the goods. Upon request from the relevant rights holder, customs must also provide information available to them of names and addresses of the consignee, the consignor and the declarant or the holder of the goods, as well as information about the origin, provenance and destination of the goods.

- If the IP rights holder confirms the IP-infringing nature of the goods as well as its agreement for their destruction, and the declarant or the holder of the goods agrees or does not reply and is deemed to have agreed, customs can proceed with the destruction.
- If one of these conditions is not met, customs release the goods to the market, unless it is notified by the IP rights holder that a legal proceeding has been initiated to establish the IP-infringing nature of the goods.

⁽¹⁰⁸⁾ [\(EU\) Regulation 608/2013 concerning customs enforcement of intellectual property rights.](#)

⁽¹⁰⁹⁾ The regulation defines the declarant as 'the person making the customs declaration in his own name or the person in whose name a customs declaration is made' and holder of the goods as 'the person who is the owner of the goods suspected of infringing an intellectual property rights or who has a similar right of disposal, or physical control, over such goods'.

The destruction of the goods is carried out under customs control and is the responsibility of the relevant IP rights holder, unless otherwise specified in the national law of the Member State where the goods are destroyed.

The regulation also establishes a **separated small consignment procedure** for goods carried by postal or express service operators⁽¹¹⁰⁾. The procedure is similar to the standard procedure but customs can destroy goods without the explicit agreement from IP rights holders in each individual case, if the relevant rights holder has opted in for such a possibility. However, before destruction, the relevant IP rights holder can request customs to provide information about the actual or estimated quantity of destroyed goods and their nature.

Under both procedures, where requested by customs authorities, IP rights holders have to reimburse the costs related to storage and destruction and may seek compensation from the infringer or other persons in accordance with the legislation⁽¹¹¹⁾. Experts pointed to the fact that under the standard procedure, the large majority of Member States requested the IP rights holder to bear the cost for destruction, and a number of Member States did the same for the small consignment procedure⁽¹¹²⁾, and that in most instances it was not possible to recover the costs from the actual IP infringers. This leads to situations where IP rights holders may decide not to request destruction of IP-infringing goods for budgetary reasons⁽¹¹³⁾.

Some experts also explained that in some instances, cases involving detained goods could be complex and lengthy, leading to situations where some T&L operators had to keep shipments stored in their warehouses for an extended period of time with no possibility of removing them or delivering them to their customers, and affecting their storage capacities and **leading to a disturbance in the supply chain**. Customs administrations in the EU have different practices, some have their own storage facilities and/or set agreements with transport and logistics operators to use their facilities, or with third parties (e.g. security firms). The choice of one storage option or the other, and the incurred costs, depend on factors such as customs resources, but also on the nature of the goods (which also affects the cost of the destruction). In that respect, experts explained that all detained shipments need to be stored in a safe and secure manner, with certain goods requiring extra care,

⁽¹¹⁰⁾ [\(EU\) Regulation 608/2013 concerning customs enforcement of intellectual property rights](#) Article 26.

⁽¹¹¹⁾ Ibid. Article 29.

⁽¹¹²⁾ [Report from the Commission to the European Parliament and Council on the implementation of the Council Regulation \(EU\) No 608/2013](#), p.15.

⁽¹¹³⁾ [2017 Situation Report on Counterfeiting and Piracy in the European Union](#), (2017, EUROPOL & EUIPO) p.45.

in particular hazardous goods. They also pointed to the fact that destruction of these types of goods are more costly than the destruction of non-hazardous goods⁽¹¹⁴⁾. Some experts highlighted the importance of cooperation within this area to try to develop secured, environmentally friendly and cost-effective ways to dispose of IP-infringing goods entering the EU.

4 Good Practices

A number of good practices already exist or are being developed to deal with some of the trends and challenges posed by the misuse of T&L services for IP-infringing activities. This discussion paper does not aim to catalogue all the good practices, but rather to establish broad categories of good practices based on concrete examples. Good practices are divided below into preventive and reactive measures in relation to IP-infringing activities.

4.1 Preventive measures

A number of good practices have been developed by T&L operators to tackle the issue of IP infringement before any real or attempted infringement occurs on their services.

4.1.1 Terms and conditions and specific policies

A number of provisions were introduced into T&L operator's terms and conditions (T&C), specifying under which circumstances the operator is able to inspect shipments. For example, in their T&C, DHL or any public authority has the right to open and inspect a shipment without notice for safety, security, customs or other regulatory reasons⁽¹¹⁵⁾. Similar provisions are included in the T&C of operators such as KLM cargo⁽¹¹⁶⁾ and UPS⁽¹¹⁷⁾. FedEx have also included a provision in their T&C, where upon the request of competent authorities, or at FedEx' discretion in compliance with applicable laws and regulations they have a right to open and inspect any shipment⁽¹¹⁸⁾. MSC's T&C

⁽¹¹⁴⁾ See section 4.2.5 on good practises regarding destruction of goods.

⁽¹¹⁵⁾ [Article 5 and section 4 of DHL Terms and Conditions.](#)

⁽¹¹⁶⁾ [section 3.6 General Conditions of KLM Cargo.](#)

⁽¹¹⁷⁾ [section 3.7 UPS Terms and Conditions of Carriage.](#)

⁽¹¹⁸⁾ [FedEx Terms & Conditions.](#)

prescribe that the maritime operator is entitled but not obliged to inspect a package at any time without giving notice to the merchant⁽¹¹⁹⁾.

4.1.2 User verification

Experts explained that many T&L companies have several measures in place to make sure they know who they are doing business with. These measures include several steps such as, verifying the legal status of their client, VAT number, legitimate bank account, previous infringements of the T&L company terms and conditions. It also includes checking the consignor and consignee against denied parties lists⁽¹²⁰⁾.

For example, DHL has put in place a ‘Denied Parties Security Screening’, that involves performing security screening on the consignor and consignee of the parcel, and running the details on the airwaybill against denied parties lists. In the case of a match, the consignor and consignee have to verify the integrity of their identity or intention of the shipment. If they are unable to do so, the shipment is stopped and sent back. In addition, DHL engages with its customers to educate and raise awareness of the importance of providing complete and accurate data, and on the tangible consequences in case of non-compliance.

4.1.3 Monitoring systems and processes

Several experts provided insights into the monitoring systems and processes put in place by some T&L operators to detect potentially bad parties and illicit goods.

- **In the air transport sector** some operators have a transparency policy on consignment data, which obliges their customer to send the consignment data in the industry standard fashion prior to acceptance by the carrier. As a consequence, no cargo or mail consignments can be accepted on behalf of the air operator until it has received the consignment data. The consignment data is then profiled by an advanced system that utilises open and undisclosed sources to match the consignment data. For instance, profiling is performed against denied

⁽¹¹⁹⁾ [Article 13 MSC Bill of Lading standard T&C.](#)

⁽¹²⁰⁾ In this paper we define denied parties lists as lists of people and/or companies that are forbidden to ship internationally issued by international government bodies such as the UN and EC. The reference also includes lists that have been compiled by the transport operators themselves.

parties lists, proprietary meta data (e.g. trigger words) and other databases to identify potential risks associated with specific consignors and/or consignees, consignment description and its routing in relation to the other elements.

A hit on a trigger word or entity will alert the operator. These alerts are classified and prioritised based on their nature (e.g. dangerous goods, military goods, live animals, IPR-infringing goods). This allows the operator to assess the risk associated with different alerts and take appropriate action when needed. These actions may include asking for additional information about the shipment or leading to a deeper investigation to decide if the shipment should be stopped or released. Where the operator decides to stop the shipment the system automatically generates a message to the warehouse management system at its origin to block the shipment. This allows the air transport operator to stop a high-risk shipment before it is loaded onto a plane, and can present a potential threat to the plane integrity. It also allows shipments that do not raise any alerts to be cleared, and get them on a 'green lane' for processing.

Experts explained that these systems could be more effective and precise in the future with the implementation of Harmonised System codes (HS codes). The HS code is an international system developed by the World Customs Organisation (WCO) to classify goods⁽¹²¹⁾. It allows economic operators, custom officials and legislators from any country to identify the same product by means of a numeric code.

The system is used by more than 200 countries⁽¹²²⁾, and as of 15 March 2021, the European Union obliged postal and express operators to provide security and safety data on the goods transported by them prior to their loading in the country of dispatch. These requirements were based on the data available in the airwaybill complemented with the appropriate HS code. The obligation to include the proper HS code lies with the customer or the entity performing customs duties on their behalf⁽¹²³⁾. One expert pointed out that if this was a requirement for the airwaybill, it would contain more detailed information about the transported goods⁽¹²⁴⁾.

⁽¹²¹⁾ The European Union uses eight-digit codes. See [Harmonised System](#).

⁽¹²²⁾ [What is the Harmonized System \(HS\)?](#).

⁽¹²³⁾ [ICAO Convention of Montreal 1999](#), paragraph 16.1 and 16.2.

⁽¹²⁴⁾ Since the EU uses eight-digit codes it will allow for a very detailed description of the goods for example down to what types of cabbage are being transported.

According to some experts, the use of HS codes and the obligation to declare the proper code for the transported goods should support profiling and identification of illicit goods and potentially contribute to detecting possible IP infringements. This is especially the case if done in combination with already existing methods for analysing and monitoring consignor- and consignee data.

- **In the maritime sector** some operators have also developed monitoring systems and processes. They rely on internal risk assessment systems, and dedicated teams to detect potential illicit goods and bad parties using their services. The system uses different risk indicators to analyse the data received by the maritime operator for each shipment, such as the type of goods, the route used, the parties involved, the documents submitted and the status of the containers. This data is analysed, and clarifications or verifications are requested by the dedicated team when needed. Once the risk assessment process is completed, the maritime operator can decide to stop the shipment or release it for transport. When a shipment is stopped, the dedicated team can also decide to investigate shipments involving the same parties to check if these should also be stopped.

An initiative has been developed by the International Chamber of Commerce (ICC) international maritime bureau (IMB) to create a register for Non-Vessel Owning Common Carriers (NVOCC)⁽¹²⁵⁾. This initiative was the result of an analysis led by IMB for its members that showed that fraudulent Bill of Ladings (B/L) were mainly originating from NVOCCs. The register was launched in January 2019 to improve anti-fraud standards and provide a mechanism to recognise NVOCCs who adhere to a minimum standard of anti-fraud measures in their operations. This in turn gives banks that specialise in trade finance (and have their own monitoring systems to prevent their services from being misused for illicit activities) the confidence that the transport documentation from the NVOCCs has been properly issued. This contributes to speeding up the clearance process for the related financial transactions.

By signing up to the register, NVOCCs are required to adopt a code of conduct⁽¹²⁶⁾, keep their contact details up to date, maintain records of previous issued B/Ls for up to 3 years and

⁽¹²⁵⁾ A NVOCC is a maritime carrier that does not have their own fleet unlike Vessel Operating Common Carrier (VOCC). This means that NVOCCs has to lease space from VOCCs that they then sell to their customers. NVOCCs transports goods under its own House BL (see section 2.1).

⁽¹²⁶⁾ [NVOCC code of conduct](#).

answer any queries from IMB related to any B/Ls they issued within 1 working day. These queries are issued by trade banks questioning the information in a B/L. In addition, participating NVOCCs commit to making every effort to ensure that any B/L they issue reflects all the facts and circumstances of the related shipments, and to take proper steps to make sure that the information in the B/L is correct. They also certify that they have the authority from or on behalf of the actual carrier to issue the B/L.

According to some experts, the register has contributed to improving the transparency and reliability of data provided by NVOCCs. Participating NVOCCs claim that they had to deal with less requests from trade banks and other parties looking to confirm shipment details⁽¹²⁷⁾.

4.2 Strengthen cooperation

A number of good practices have also been developed by T&L operators, IP rights holders and LEAs to counteract actual or attempted misuses of T&L services for IP-infringing activities.

4.2.1 Cooperation between T&L operators and IP rights holders

Different initiatives have been developed to improve the cooperation between T&L operators and IP rights holders, and notably to the sharing of information and the enhancement of risk profiling systems.

- A **cross industry working group (CIWG)**, with private companies in the fields of luxury goods, tobacco, car manufacturing and agrochemical and life sciences has established a collaboration initiative with some of the main maritime operators. The cooperation aims to prevent the transport of illicit goods, by providing input to enhance existing risk profiling systems from transport operators, but also by creating and sharing algorithms to implement or enhance these systems.

This collaboration has already resulted in promising outcomes, such as enhanced and targeted risk profiling, and the identification of loopholes that have the potential or have already been exploited by criminals. In this context, some experts pointed to the opportunity to extend this

⁽¹²⁷⁾ [Article](#) on ICC website.

collaboration to other transport sectors and intermediaries, as well as to other IP rights holders and opening it up to LEAs. One of the next steps envisioned is the creation of a forum or a platform supporting the secure exchange of information between the different stakeholders, in full compliance with all applicable regulations.

- **Declaration of intent to prevent the maritime transportation of counterfeit goods⁽¹²⁸⁾:** several trade associations, private companies and maritime operators signed this declaration, which was facilitated by the Business Action to Stop Counterfeiting and Piracy (BASCAP) initiative of the ICC in 2016. The signatories of the declaration recognised the destructive impact of the international trade in counterfeiting and agreed to develop a ‘detailed series of non-binding measures or best practices’ to be implemented in relation to a set of principles. These principles included a zero tolerance regarding counterfeits⁽¹²⁹⁾, the application of supply chain controls⁽¹³⁰⁾, and risk profiling by maritime operators, with a cooperation from the signatories to review and refine these systems. They also included raising awareness on the consequences of counterfeiting and training of employees from the transport sector to report suspected counterfeit activities⁽¹³¹⁾, as well as sharing of information and collaboration between the signatories on detection and detention of counterfeit products⁽¹³²⁾.

Some IP rights holders are also developing specific agreements with transport operators and fulfilment centres, to tackle new methods used by IP infringers to lower the risks of detection of their products throughout the distribution chain⁽¹³³⁾.

4.2.2 Cooperation between LEAs, IP rights holders and T&L operators

⁽¹²⁸⁾ See ICC BASCAP [Declaration of intent to prevent the maritime transportation of counterfeit goods](#), November 2016.

⁽¹²⁹⁾ Zero tolerance policy encompasses a commitment to implement and ensure compliance with applicable international, regional and national rules and mutually agreed standards aimed at preventing the carriage of counterfeit products. Furthermore, it includes commitment to inform all customers and sub-contractors of these commitments and our zero-tolerance policy towards counterfeits.

⁽¹³⁰⁾ Such as ‘Know Your Customer’ and other due diligence measures to stop business with those dealing in the counterfeit trade, as well as the commitment to include appropriate conditions prohibiting the carriage of counterfeit products.

⁽¹³¹⁾ Increase awareness about the nature, scale, and consequences of counterfeiting and improve the training of staff within the transport sector to enable them to report suspected counterfeit activity.

⁽¹³²⁾ Furthermore, commitment to cooperate and collaborate with competent law enforcement authorities on any investigations relating to the carriage of counterfeits.

⁽¹³³⁾ [Canon USA successfully stops a new method of importing counterfeit goods into the US.](#)

The **IP enforcement portal (IPEP)**⁽¹³⁴⁾ is a free platform developed by the EUIPO, that serves as a secured communication tool between rights holders (and/or their legal representatives), EU Customs Authorities, MS Police Authorities, MS Market Surveillance Authorities, EU Judiciary Authorities, EUROPOL, OLAF and DG TRADE. It is predicted that the platform will be open to other relevant parties such as intermediaries, notably e-commerce marketplaces⁽¹³⁵⁾, and third country enforcement authorities in the near future.

The **IPEP exchange module** allows a real time exchange between rights holders and enforcement authorities related to IPR related matters. The module has several functionalities such as rights holder alerts to enforcement authorities related to potential online and offline infringements and trends that they have noticed. These alerts can then be shared by the authorities to other authorities warning them about a specific situation, trend or threat. They can also share interesting cases they have had with other enforcement authorities. In turn, enforcement authorities can send notifications to rights holders on suspicious goods they have detected, detention of goods in the internal market or at the boarder (this functionality is still in its pilot phase). In addition, IPEP allows authorities to search for information about valid IP rights, companies, products (specific information submitted by rights holders about their products), contact points for rights holders and filed Applications for Actions (AFA)⁽¹³⁶⁾.

IPEP also allows rights holders and their representatives to file AFAs to customs through the system, on a voluntary basis. Since 13 December 2021 all these applications must be filed and managed electronically.

The **IPEP detentions module** allows enforcement authorities (at the border and in the internal market) to share statistical information on their detentions of IPR-infringing goods. This information can be uploaded to the system in bulk and contains details such as product type, place of detention, number of items detained, estimated retail value and, in the case of border detention, link to the AFA.

In addition to the above functionalities, IPEP has a **non-EU case module**. This module collects data reported by rights holders on IPR infringement cases that they have been involved in outside of the

⁽¹³⁴⁾ See [IP Enforcement Portal webpage](#).

⁽¹³⁵⁾ See EUIPO's strategic project on [Enhancing IP protection on E-commerce marketplaces](#). The first phase in this project was to create a [web page](#) listing different marketplace IP protection tools. The second phase will be to allow marketplaces access to IPEP where they will be able to verify IPRs and contact rights holders.

⁽¹³⁶⁾ See section 2.8.1.

EU as well as the measures local enforcement authorities have taken after being notified by the rights holders.

Another example of cooperation between LEAs and private companies can be found in the United Kingdom (UK) where, Her Majesty's Revenue and Customs, Border Force officials with support from UK Trading Standards, the Anti-Counterfeit Group⁽¹³⁷⁾, and the UK IP Office (UKIPO) regularly **run 'intensification exercises'** to detect counterfeits in postal traffic at freight cargo depots and courier hubs located at major airports within the UK. Each day during the exercise, and if and when the border force detain any parcels, they notify the anti-counterfeit group and rights holders of all detentions made that day. Rights holder representatives then examine the goods detained in person and make an assessment of the authenticity and any counterfeit items are detained. The volumes of counterfeits detained during these exercises have ranged from 6 000 to 35 000 items. Intelligence from these intensification exercises is collected with a view to generating inland enforcement actions against those importing and supplying counterfeit goods. These intensification exercises also increase collaboration and coordination between rights holders and the authorities.

Some T&L operators are also developing specific cooperation with LEAs. For example, DHL has developed a global customs compliance programme⁽¹³⁸⁾ that identified and targets four risk areas: IPR infringement, undervaluation of goods and misdeclaration of information related to the goods, shipper and receiver. This programme has resulted in a MoU⁽¹³⁹⁾ between DHL in Hong Kong and Hong Kong customs related to the exchange of information, especially targeting IPR-infringing goods. The first couple of years resulted in a notable increase of detentions of illicit shipments by Hong Kong Customs, and the collaboration is still ongoing⁽¹⁴⁰⁾.

⁽¹³⁷⁾ The [Anti-counterfeit Group](#) represents more than 3 000 brands in 30 countries.

⁽¹³⁸⁾ [Global Customs Compliance Programme](#).

⁽¹³⁹⁾ [Memoranda of Understanding](#).

⁽¹⁴⁰⁾ [Article](#) on WCO website.

4.2.3 Cooperation between LEAs

A number of initiatives are developing at national, regional and global levels to further the cooperation between LEAs.

- **At a national level – establishment of one-stop-shop inspection centres:** for example in the Netherlands, the custom administration has developed Joint Inspection Centres (JIC) at both the Port of Rotterdam and Schiphol International Airport. At these centres, different control agencies, such as the Netherlands food and consumer product safety authority, closely cooperate with customs to check air cargo. If necessary, the cargo is unpacked at the JIC, (in the presence of the shipper) and all the control agencies involved in the cooperation carry out their respective controls simultaneously.
- **At a regional level – cooperation between different national customs authorities:** for example, the customs eastern and south-eastern land border expert team (CELBET) initiative⁽¹⁴¹⁾, has brought together customs authorities from 11 EU Member States⁽¹⁴²⁾ since 2016, and works under the EU 2020 customs programme⁽¹⁴³⁾. The main objective of the initiative is to strengthen and improve the operational cooperation through real operational coordination, deeper sharing of information and pooling of human resources contributing to the implementation of a common customs legislation and policy.

The joint team is working under the supervision of the European Commission Directorate General for Taxation and Customs Union (DG TAXUD), and its various project teams cooperate to achieve greater synergies between different activities performed by customs at road/rail border crossing points. The team notably provides solutions for better risk assessment, uniform performance measurement standards, flexible use and sharing of resources, training of customs officers, interaction and coordination with relevant border services (including those of neighbouring third countries). It also supports Member States with expertise and technical requirements of customs control equipment.

⁽¹⁴¹⁾ [CELBET](#).

⁽¹⁴²⁾ Finland, Estonia, Latvia, Lithuania, Poland, Hungary, Slovakia, Croatia, Romania, Bulgaria and Greece.

⁽¹⁴³⁾ [\(EU\) Regulation 1294/2013 on establishing an action programme for customs in the EU for the period 2014-2020](#), Article 7(a)(v). Please note that the new [EU 2027 Customs programme](#) has now come into effect.

CELBET helps to improve the control of external borders preventing the entry of dangerous goods that could be harmful to people, to the environment or to the EU and its Member States and its citizen's financial interest. The improved control also contributes to smoother and faster border crossing of citizens and goods.

- **At an EU level** – the European anti-fraud office (OLAF) supports Member States in their efforts to detect and combat IPR infringements that puts citizens' health and safety at risk⁽¹⁴⁴⁾. OLAF also makes available a set of IT applications under the anti-fraud information system to support the exchange of information on IPR for anti-fraud purposes. This includes the anti-fraud transit information system (ATIS), which contains information on movements of goods under the common transit procedure, the container status messages (CSM) directory that records movements of maritime containers that enter or leave the EU territory, the virtual operations coordination unit (VOCU), an IT application for the secure exchange of information during operational actions, and the customs information system (CIS) for the exchange of information between EU Member States and the EC on suspicious goods and/or detentions of counterfeit goods. The CIS is connected with DG TAXUD's COPIS system and the customs enforcement network (CEN) of the World Customs Organisation (see below).

OLAF and the EUIPO has recently signed a service level agreement providing for, inter alia, the development of an IT tool to allow for the automated transfer of data on detentions of counterfeit goods between Member States national customs system and the CIS. This IT tool will contribute to the development of a single-entry point for all data related to IP crime under the framework of the EUIPO technical group on IP enforcement and data exchange. The newly signed agreement also covers organisation of specific events, such as training activities, seminars and information sessions, all related to the fight against IPR infringements in support of operational activities carried out by OLAF and EU Member States. Furthermore, the agreement also opens up the possibility to conduct joint strategic analysis and data exchanges between OLAF and the EUIPO.

- **At a global level – global intelligence network:** as part of its objectives, the World Customs Organisation (WCO) aims to support the exchange of intelligence among all stakeholders. In

⁽¹⁴⁴⁾OLAF uses several systems and applications that allow them to obtain crucial information to detect suspicious shipments of goods infringing IPR.

this context it has established a set of regional intelligence liaison offices (RILOs)⁽¹⁴⁵⁾ with the intention of creating a global intelligence network. Among the WCO tools used by the RILOs' network is the WCO **customs enforcement network** (CEN)⁽¹⁴⁶⁾, which is a global database containing customs detention information, and the CENcomm, a web-based communication system allowing a closed user group to exchange messages for the duration of an operation or project. The RILOs' network often uses the CEN database to analyse detentions and develop regional intelligence products, while the CENcomm platform serves to exchange operational information and facilitate real-time secure communications among members and partners.

The exchange of intelligence has a multi-level approach.

- **At a national level:** member administrations' National Contact Points (NCPs) gather information on detentions made from existing sources and input the data into the CEN. They also analyse the information collected at the national level to identify new trends, produce alerts and transmit them to the RILOs' they are working with, for regional circulation.
- **At a regional level:** the RILOs study and evaluate international detentions, verify the accuracy of the CEN data supplied by the NCPs, prepare and circulate alerts and intelligence profiles. They also organise and support regional intelligence-based operations, facilitate mutual assistance and co-operation with other law enforcement services, and provide technical or other assistance to NCPs.
- **At an international level:** the WCO Secretariat is responsible for the central management of the CEN, operating and maintaining the system as a global information and intelligence tool for the RILOs' network. Building on the information gathered in the CEN, the secretariat periodically conducts global strategic and tactical analyses, circulating a summary of its analyses in its annual reports, offering training and technical assistance to the RILOs and their members, and sharing strategic information with other international organisations engaged in combating organised crime.

⁽¹⁴⁵⁾ [RILO offices](#).

⁽¹⁴⁶⁾ [customs enforcement network](#).

On the 7 June 2021, the WCO and OLAF signed an administrative cooperation arrangement (ACA), in order to strengthen their cooperation in the fight against IPR infringements. The ACA opens up for the possibility (started in March 2022) to transfer non-personal data of relevant customs information system (CIS) cases related to suspicious goods and/or detentions of counterfeit goods into the CEN. This possibility is consistent with the principle of ‘one detention, one report’ and reduces the administrative burden by allowing Member States’ national customs authorities to enter detention data only once in the CIS and that a non-nominative set of this data could be automatically transferred to the CEN. This process avoids multiple entries of data by customs officers and reduces the risk of errors.

Another example of cooperation is the **WCO-UPU Contact Committee**⁽¹⁴⁷⁾. The committee was established in 1965 and acts as a working group whose conclusions are submitted to the competent WCO and UPU bodies for approval. The committee comprises 16 experts with eight experts from different custom administrations and eight experts from different postal operators. The committee deals with issues of common interest and, in particular, seeks to speed up and simplify customs formalities in the postal service. The committee have several workstreams including, to facilitate and simplify customs formalities, to promote and ensure transport of legitimate trade through the postal network, to develop standards and tools (e.g. for exchange of data) and specific exchange of data related to common issues such as issues related to clearance of postal items. They also conduct awareness raising and operational activities in different areas, such as IPR.

4.2.4 Cooperation between different types of intermediaries

As mentioned by some experts the sharing of information between T&L operators and other types of intermediaries is a real challenge and opportunity (see section 3.2.1). Experts pointed to the Electronic Commerce Working Group (ECWG) formed by the US government in 2017, which brought together online sales platforms, express delivery companies and payment processors. The goal of the ECWG was to enhance data sharing among different types of intermediaries, as well as ‘competitors’ in the same sector and, ultimately, with LEAs to increase existing efforts to identify,

⁽¹⁴⁷⁾ [WCO-UPU Contact Committee](#). On 9 May 2022 a new cooperation agreement was signed between WCO and UPU. The new cooperation agreement intends to replace the existing Memorandum of Understanding (MoU) originally signed by the WCO and the UPU in 1994 and amended in 2007, in order to reflect the recent regulatory and technology developments and adequately respond to the rapid growth of international mail volumes stemming from e-Commerce.

investigate, and take-down sellers of IPR-infringing goods and hold them accountable. Since its inception, online sales platforms involved in the working group have participated in a pilot data-sharing project facilitated by the US National Intellectual Property Rights Coordination Centre. The pilot project, conducted throughout 2020, validated the concept that a robust exchange of data is an effective way to identify common targets and actionable intelligence for both the private sector and LEAs and documented the following:

- during the pilot project, the participating stakeholders shared information on a regular basis and in every instance cross-platform illicit activity was found;
- a review of the combined datasets indicated that the same individual/business used different/multiple IP addresses, business names, business addresses and phone numbers;
- sellers of IP-infringing goods were also targeted in criminal/civil litigation suits for trade mark/copyright violations and other illicit activity, including wire fraud and money laundering;
- multiple targets were the subject of Department of Homeland Security investigations and detentions.

Building on the pilot project, the ECWG identified a third-party vendor to work on building, testing, and managing a data sharing platform in 2021 and will continue its efforts to formalise and expand data-sharing in the future.

4.2.5 Destruction of IPR-infringing goods

Experts highlighted a few initiatives from the private sector in regard to storage and destruction of IPR-infringing goods and how they deal with this.

- Some anti-counterfeiting organisations support their members in the fight against counterfeits, assisting them in providing customs with relevant paperwork (e.g. application for actions or AFA) to request that they monitor and detect infringing goods⁽¹⁴⁸⁾. They also provide advice on how to follow up with customs when goods have been detained.

These organisations can also help their members to dispose of detained goods. In many cases, the cost of storage and destruction is the responsibility of the IP owner, and acts as a

⁽¹⁴⁸⁾ See section 2.8.1.

deterrent for IP rights holders to take action (see section 3.2.3). In this context, some anti-counterfeiting organisations are working on more sustainable and cost-effective solutions to dispose of IPR-infringing goods⁽¹⁴⁹⁾.

In this context experts explained that beyond the environmental benefits, the development of these initiatives could help IP rights holders to save money on destruction, and allow them to request actions from customs in a larger number of cases⁽¹⁵⁰⁾.

- E-commerce marketplaces are also taking action to detain and destroy IPR-infringing goods. These programmes can lead to the take down of listings for IP-infringing goods, and suspension or termination of the related sellers account, but also, when the goods are held in e-commerce market place fulfilment centres, for their destruction. For example, according to Amazon 2021 Brand Protection Report⁽¹⁵¹⁾, in 2020 it managed to detain and destroy over 2 million counterfeited products before they were sent to consumers.

5 New Technical Solutions Currently Considered or Developed

As explained throughout this discussion paper, T&L is a fast changing and innovative ecosystem. Different operators implement new technical solutions to comply with regulatory requirements, limit their risks, but also provide solutions to clients for them to be able to monitor and secure their supply chains. In this context, a number of technical solutions that can counteract the misuse of T&L services for IP-infringing solutions are being considered or are under development.

5.1 Tracking devices

⁽¹⁴⁹⁾ For example, the [REACT Sustains](#) initiative aims at destroying detained goods in an effective and sustainable way. This initiative is a collaboration between REACT and Dutch Customs in which IP-infringing goods detained by customs in the Netherlands, Belgium and Germany are brought to storage facilities in the Netherlands, where they are processed, dismantled, and made available for recycling.

⁽¹⁵⁰⁾ According to [REACT](#) the initiative has showed an estimated saving of 40 % compared to when goods are destroyed in the traditional manner.

⁽¹⁵¹⁾ [2021 Brand Protection Report](#).

Experts explained that beyond monitoring distribution chains, modern tracking devices could also help counteract a practice from illicit traders, including IP infringers, which compromises the integrity of containers transporting perfectly legitimate goods to add their illicit goods. In this context, they pointed to the development of smart trackers supporting the tracking of containers in real time with exact geolocation, status, transport conditions and analytics of the cargo.

These systems allow to identify exactly when, where, and why disruptions and delays occur, and experts explained that they could also detect when a container was tampered with, by detecting if a container was opened during transit and for how long, or monitoring temperature changes and shocks. Some experts suggested that the generalisation of this equipment would contribute to counteract the tampering of containers to transport illicit goods.

5.2 Blockchain based solutions

The use of blockchain technology is explored to streamline the process of supply chain paperwork, identification of IP-infringing goods and tracking of origin, building on the main features of this technology that include immutability, decentralisation, driven by consensus, and transparency.

5.2.1 Blockchain based solutions developed by private sector

There are a number of blockchain based solutions that have been initiated by the private sector. Some of these solutions have the same purpose and are used in the same sector and sometimes even interact with each other. However, most of them are tailored to the needs of a specific business and work independently of others.

Some solutions have been developed to help with the optimisation of supply chain management and business processes for its users, such as the blockchain platform VeChain⁽¹⁵²⁾. The Blockchain in Transport Alliance BiTA⁽¹⁵³⁾ is another project whose members focus on the adoption of blockchain technologies in supply chain management. Other solutions focus on using blockchain for authentication and track and trace services. As mentioned, although these solutions have similar

⁽¹⁵²⁾ [VeChain](#).

⁽¹⁵³⁾ [BiTA](#).

purposes they are normally customised to accommodate users' special needs and requirements⁽¹⁵⁴⁾.

Other solutions are aimed at making transportation more efficient, equitable, decentralised, and sustainable but also for the exchange of reliable shipping information and interaction between various operators and customs authorities⁽¹⁵⁵⁾.

5.2.2 Blockchain based solutions driven by the public sector

While there are many private initiatives developing, notably to authenticate and track products, they tend to work in silos with no possible way to interconnect these different solutions throughout the supply chain⁽¹⁵⁶⁾, which counterfeiters use to their advantage. In an attempt to overcome this issue, the EUIPO has been working on a pilot project for a blockchain-based system that would interconnect all the interested parties and their systems to ensure product authenticity throughout the whole supply chain, and eventually beyond.

As part of this pilot project, the infrastructure itself will be developed through collaboration with various stakeholders, united under the Blockathon Forum⁽¹⁵⁷⁾. The EUIPO solution would provide them with the means to transfer a product together with its virtual equivalent (a Non-Fungible Token), the latter being stamped with an immutable digital anti-counterfeiting label. It will not compete with existing solutions such as Non-Fungible Tokens (NFT) platforms, private or public blockchain track and trace solutions or existing and digitally enabled product ID serialisation. Instead, it will leverage them in order to guarantee that the product is genuine and its current holder is identified.

Importantly, during the whole product journey, organisations and product holders will be identified through a trust register built and maintained by the EUIPO, which will also leverage pre-existing databases and enforcement tools⁽¹⁵⁸⁾. Specifically for the first block, this global chain, the EUIPO register would guarantee rights holders' identification and validate their capacity to create anti-counterfeiting labels. Using a standardised data structure, the solution would then allow logistic

⁽¹⁵⁴⁾ See for example, [Arc-Net](#), [Morpheus](#), [IOTA](#) and [Everledger](#).

⁽¹⁵⁵⁾ See for example, [MOBI](#), [FedEx](#), [Linux](#) and [Maersk](#) and [IBM](#).

⁽¹⁵⁶⁾ EU intellectual property offices, governments, customs authorities, manufacturers, transport and logistics operators, intermediaries, and retailers.

⁽¹⁵⁷⁾ [Blockathon Forum](#).

⁽¹⁵⁸⁾ Such as [TMview](#), [DesignView](#), [IPEP](#) and [IP Register in Blockchain](#).

operators, freight forwarders and other carriers to interact in the logistics nodes via scan events, until the product reaches the retailer or the end consumer. Additionally, the solution aims to interconnect with the risk analysis systems of interested enforcement authorities, possibly to improve current alert mechanisms as well as product green lanes at border crossings.

The EUIPO expect to release a first version of the solution by the end of 2023, and, in the long term, ideally scale up and evolve in order to connect to the European Blockchain Service Infrastructure⁽¹⁵⁹⁾ and the European Self-Sovereign Identity Framework⁽¹⁶⁰⁾.

6 Conclusions

The T&L ecosystem encompasses a broad variety of operators that are taking part in large supply chains, and are using different systems to gather and share information with public authorities, in particular customs. IP infringers use a number of tactics to defeat control measures of public authorities and T&L operators and move their illicit goods undetected throughout the supply chain.

Experts have pointed out several challenges to counteract this misuse, and they have also identified several good practises with T&L operators cooperating with each other, LEAs and rights holders, as well as technical solutions that already exist or are being developed.

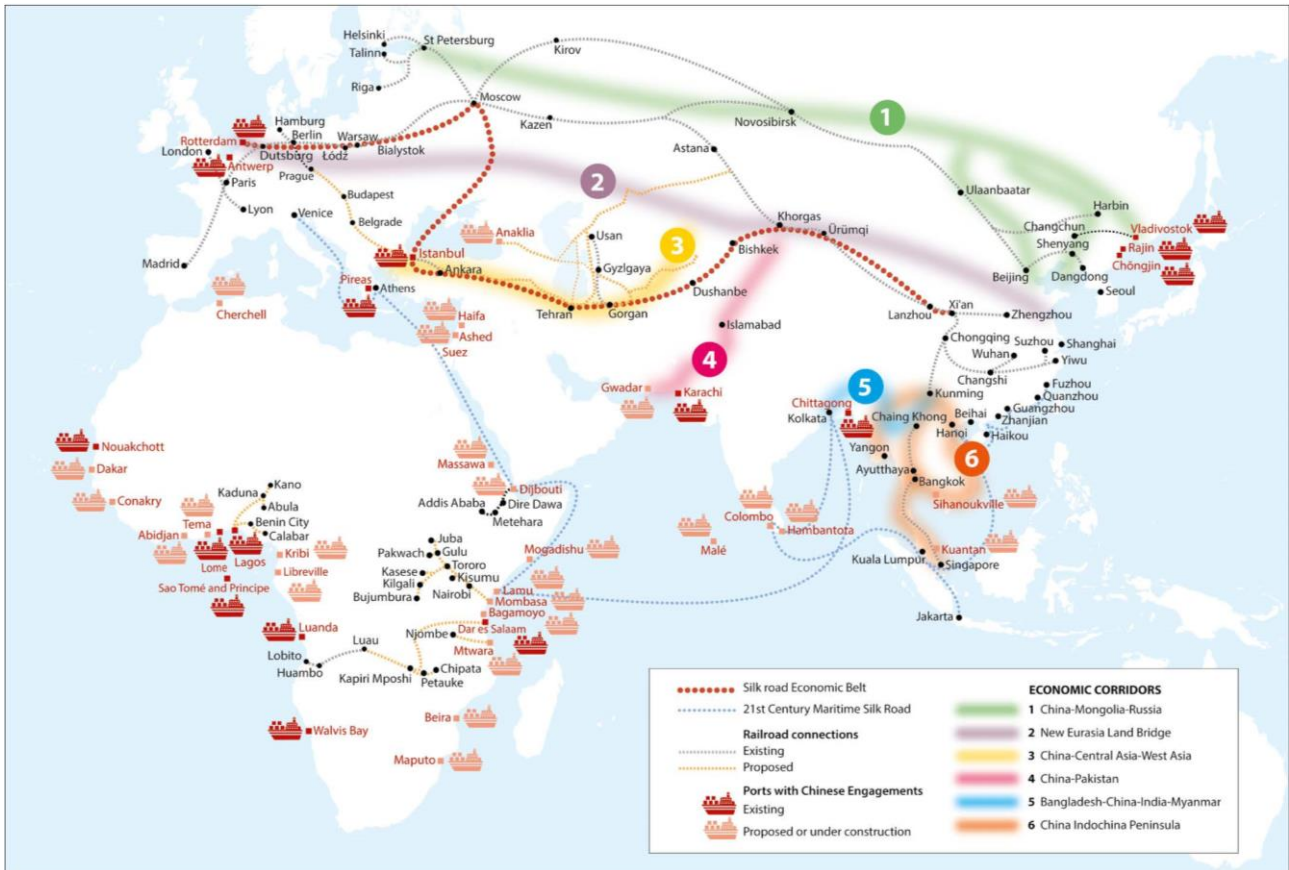
This discussion paper will hopefully contribute to a better understanding of the very complex innovative, and fast changing T&L ecosystem and to the discussions on ways to enhance cooperation and develop technology for all the relevant operators to jointly tackle the misuse of different T&L services for IP-infringing activities.

⁽¹⁵⁹⁾ [European Blockchain Service Infrastructure.](#)

⁽¹⁶⁰⁾ [European Self-Sovereign Identity Framework.](#)

Annexes

Annex 1 – Belt and Road Initiative



Annex 1 OECD (2018), 'The Belt and Road Initiative in the global trade, investment and finance landscape', in OECD Business and Finance Outlook 2018, OECD Publishing, Paris, https://doi.org/10.1787/bus_fin_out-2018-6-en.

TRANSPORT AND LOGISTICS – DISCUSSION PAPER
Challenges and good practices for transport and logistic services
to prevent the use of their services for IPR-infringing activities

ISBN 978-92-9156-325-8 DOI 10.2814/719443 TB-07-22-871-EN-N

© European Union Intellectual Property Office, 2022

Reproduction is authorised provided the source is acknowledged