Council of the European Union

Brussels, 29 September 2021
(OR. en)

12353/21

LIMITE

JAI 1035
FRONT 345
ASIM 76
MIGR 209
CATS 58
COPEN 364
COSI 177
CRIMORG 83
ENFOPOL 337

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Digitalisation of migrant smuggling

Delegations will find enclosed a report from Frontex and Europol on “Digitalisation of migrant smuggling”.

FRONTEX

EUROPEAN BORDER AND COAST GUARD AGENCY

EUROPOL

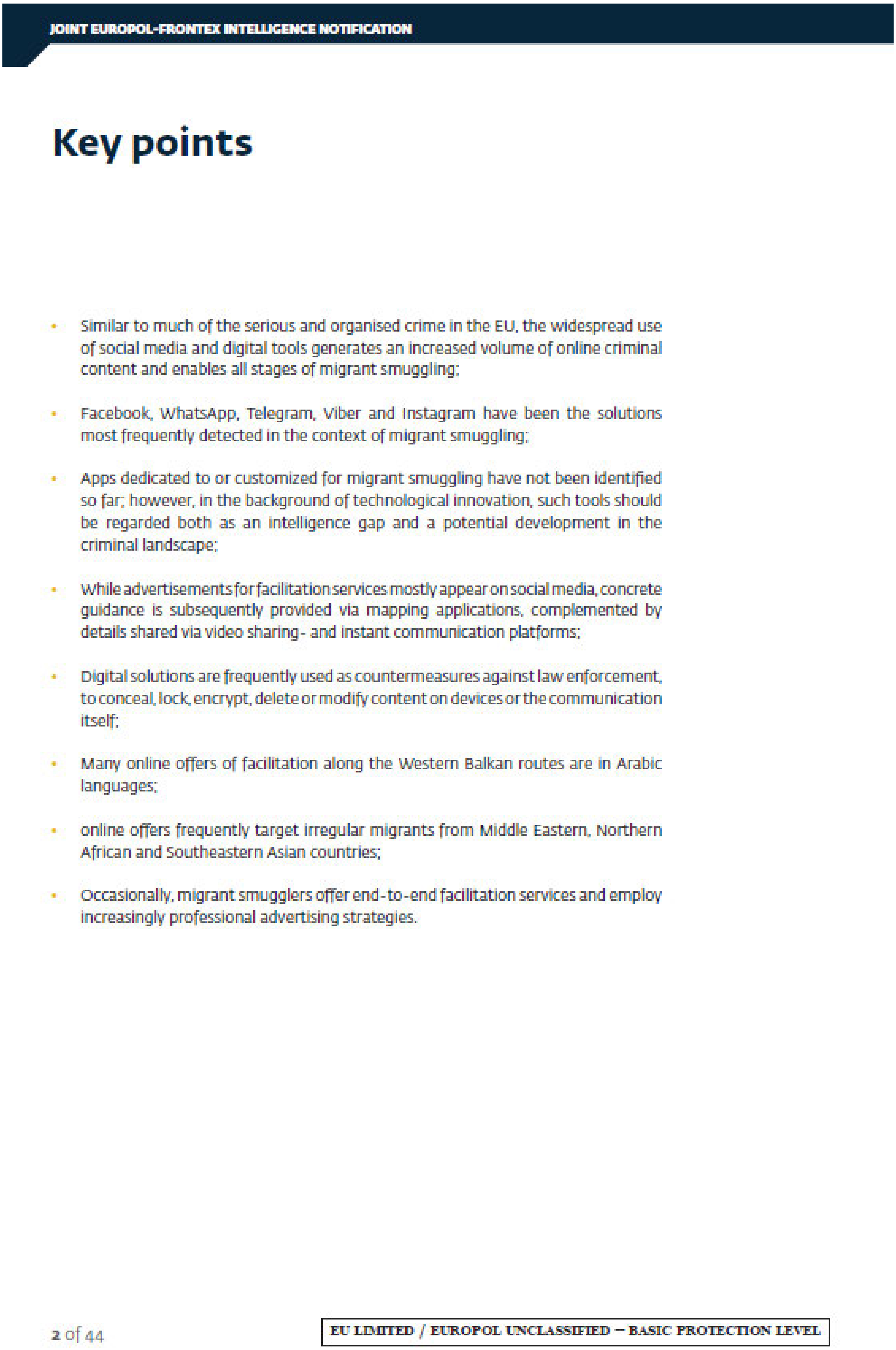
Digitalisation of migrant smuggling

Digital tools and apps enabling facilitation

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL

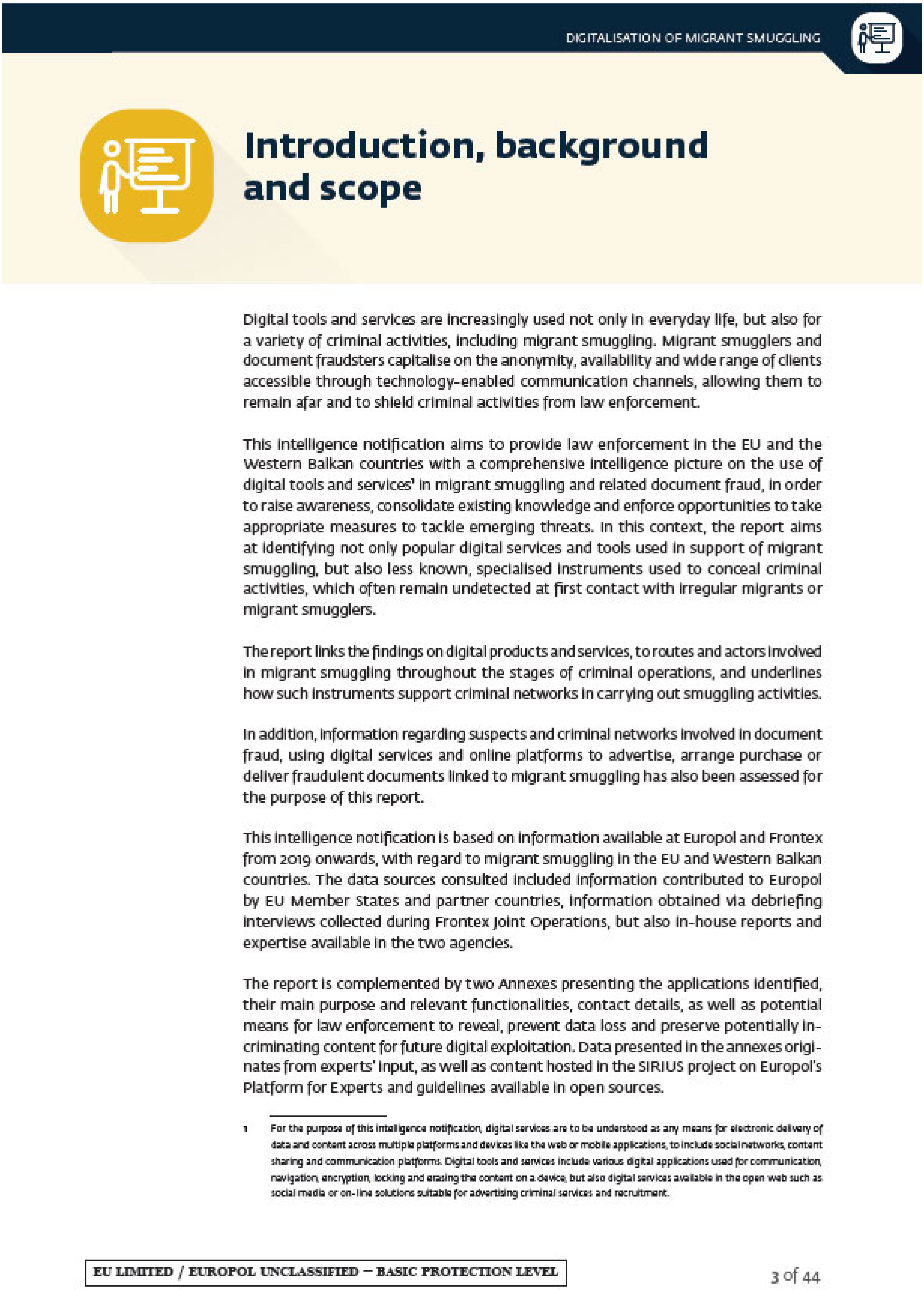
Table of contents

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL



Key points

- Similar to much of the serious and organised crime in the EU, the widespread use of social media and digital tools generates an increased volume of online criminal content and enables all stages of migrant smuggling;
- Facebook, WhatsApp, Telegram, Viber and Instagram have been the solutions most frequently detected in the context of migrant smuggling;
- Apps dedicated to or customized for migrant smuggling have not been identified so far; however, in the background of technological innovation, such tools should be regarded both as an intelligence gap and a potential development in the criminal landscape;
- While advertisements for facilitation services mostly appear on social media, concrete guidance is subsequently provided via mapping applications, complemented by details shared via video sharing- and instant communication platforms;
- Digital solutions are frequently used as countermeasures against law enforcement, to conceal, lock, encrypt, delete or modify content on devices or the communication itself;
- Many online offers of facilitation along the Western Balkan routes are in Arabic languages;
- online offers frequently target irregular migrants from Middle Eastern, Northern African and Southeastern Asian countries;
- Occasionally, migrant smugglers offer end-to-end facilitation services and employ increasingly professional advertising strategies.



Introduction, background and scope

Digital tools and services are increasingly used not only in everyday life, but also for a variety of criminal activities, including migrant smuggling. Migrant smugglers and document fraudsters capitalise on the anonymity, availability and wide range of clients accessible through technology-enabled communication channels, allowing them to remain afar and to shield criminal activities from law enforcement.

This intelligence notification aims to provide law enforcement in the EU and the Western Balkan countries with a comprehensive intelligence picture on the use of digital tools and services[1] in migrant smuggling and related document fraud, in order to raise awareness, consolidate existing knowledge and enforce opportunities to take appropriate measures to tackle emerging threats. In this context, the report aims at identifying not only popular digital services and tools used in support of migrant smuggling, but also less known, specialised instruments used to conceal criminal activities, which often remain undetected at first contact with irregular migrants or migrant smugglers.

The report links the findings on digital products and services, to routes and actors involved in migrant smuggling throughout the stages of criminal operations, and underlines how such instruments support criminal networks in carrying out smuggling activities.

In addition, information regarding suspects and criminal networks involved in document fraud, using digital services and online platforms to advertise, arrange purchase or deliver fraudulent documents linked to migrant smuggling has also been assessed for the purpose of this report.

This intelligence notification is based on information available at Europol and Frontex from 2019 onwards, with regard to migrant smuggling in the EU and Western Balkan countries. The data sources consulted included information contributed to Europol by EU Member States and partner countries, information obtained via debriefing interviews collected during Frontex Joint Operations, but also in-house reports and expertise available in the two agencies.

The report is complemented by two Annexes presenting the applications identified, their main purpose and relevant functionalities, contact details, as well as potential means for law enforcement to reveal, prevent data loss and preserve potentially incriminating content for future digital exploitation. Data presented in the annexes originates from experts' input, as well as content hosted in the SIRIUS project on Europol's Platform for Experts and guidelines available in open sources.

[1] For the purpose of this intelligence notification, digital services are to be understood as any means for electronic delivery of data and content across multiple platforms and devices like the web or mobile applications, to include social networks, content sharing and communication platforms. Digital tools and services include various digital applications used for communication, navigation, encryption, locking and erasing the content on a device, but also digital services available in the open web such as social media or on-line solutions suitable for advertising criminal services and recruitment.

Migrant smuggling in the digital era

The digital transformation of society as a whole has had a fundamental impact on serious and organised crime in the EU, virtually all criminal activities now featuring an online component.[2] Migrant smuggling makes no exception. Digital services and tools are increasingly used by criminal networks capitalising on the opportunity to steer criminal activities from afar, by opportunistic individuals, providing facilitation services on an ad-hoc basis, but also by irregular migrants, upon indications from smugglers.

Free and popular solutions like Facebook, Instagram, Signal, Skype, Telegram, Viber, WhatsApp and Twitter are most frequently detected and reported in relation to migrant smuggling, while more specialised tools are also used to shield operations or deter law enforcement action, by locking or disguising content, erasing data or providing anonymous internet connection. Mapping applications and open geographic data sources such as Maps.me and Google maps are key tools used by smugglers to share maps, routes, coordinates, waypoints and placemarks[3], and other details to support irregular migrants in finding their way without direct contact. Reported with a smaller frequency, channels such as VK and OK.RU, WeChat, Zalo or Azar, may be used preferably by smugglers and irregular migrants operating or originating from certain geographic areas outside of the EU (Russian Federation and Ukraine, China, Vietnam etc.).

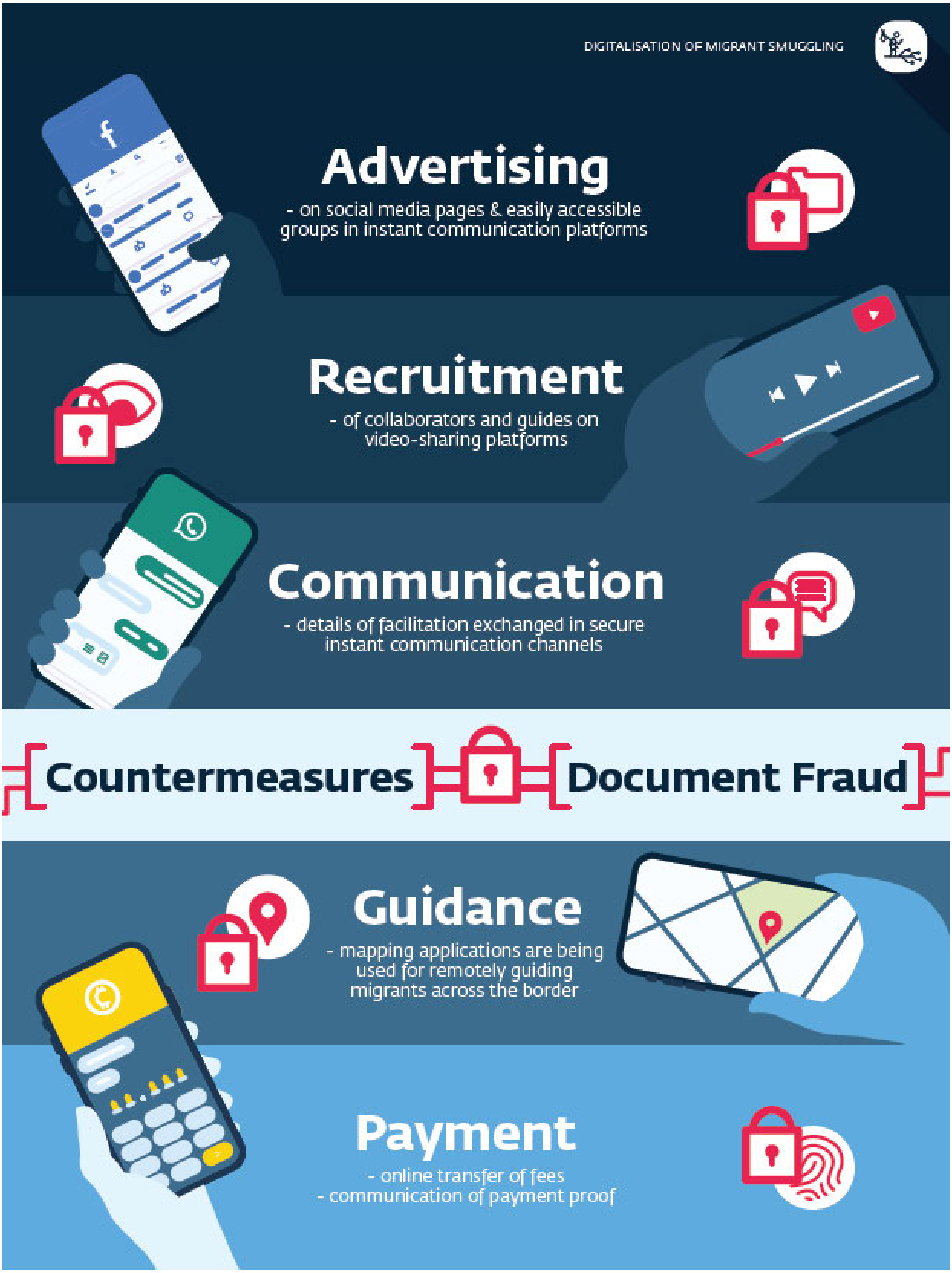
Other platforms like WICKR or ICQ were also reported in connection to sharing directions and pick-up points for irregular migrants or, respectively, for provision of forged documents, but their incidence is also lower.

A large share of Europol's information on the use of digital solutions for migrant smuggling points towards Albanian, Syrian, Pakistani, Iraqi, Afghan and Moroccan smugglers, facilitating Middle Eastern, East Asian and African irregular migrants via the Eastern Mediterranean route and then through variations of the Western Balkan routes into the EU, by foot, in trucks or trailers. Fewer reports were received concerning smugglers facilitating irregular migrants via the EU's Eastern borders, from Belarus, Russia and Ukraine, via Poland, and further to other EU MS.

Opportunities offered by the online environment and widely available digital tools are thoroughly exploited in all stages of migrant smuggling: from advertising and recruitment of clients or low level facilitators, to communication with irregular migrants or among smugglers, sharing travel guidance, provision of fraudulent documents and enforcement of countermeasures against law enforcement.

[2] Europol, 2021, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA) 2021 – A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime [April 2021] accessible at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

[3] A waypoint is an intermediate point along a route, a kind of colour-coded placemark; A placemark marks a position on the Earth's surface, using a colored pushpin as the icon. https://developers.google.com/kml/documentation/kml_tut#placemarks.



DIGITALISATION OF MIGRANT SMUGGLING

Advertising

- on social media pages & easily accessible groups in instant communication platforms

Recruitment

- of collaborators and guides on video-sharing platforms

Communication

- details of facilitation exchanged in secure instant communication channels

Countermeasures

Document Fraud

Guidance

- mapping applications are being used for remotely guiding migrants across the border

Payment

- online transfer of fees
- communication of payment proof

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL

Advertisement and recruitment

Online advertisement of smuggling services appears to become increasingly professional, with criminals using several platforms in parallel, updating information regularly or sharing videos, reviews and testimonials on successful operations. Smuggling services are heavily advertised on social media platforms, particularly Facebook or Instagram pages, but recently also TikTok. Advertisement is carried out on personal profiles or generic/business pages[4], but also on chat groups in messaging platforms like Whatsapp or Telegram. In addition to freely available and open channels for advertisement, fewer cases of smugglers using the Darkweb to offer their services were also reported.

Social media pages, groups and platforms offering smuggling services contain instructions, maps, photos, videos and prices for smuggling, updated on a regular basis. Occasionally, the content posted by smugglers is complemented by information contributed by numerous other users, in the form of comments or notifications. Groups and pages hosting advertisement for smuggling are easily searchable by keywords, as the names include combinations of relevant words such as immigration, asylum, visa, smuggling, or refer to the routes for which facilitation is advertised – e.g. "Immigrate to Canada, Europe, UK". Most often though, advertisement on social media only contains basic information and contact details leading to private groups in instant communication platforms, through which the terms of the facilitation are subsequently discussed and agreed.

Both smuggling from countries of origin and facilitation of secondary movements through the EU are advertised online. Most often, criminals advertise facilitation along the Eastern Mediterranean route and the Western Balkan routes, through countries like Albania, Bulgaria, Greece, North Macedonia and Serbia, further towards EU MS or, in some cases, towards third countries like the UK, the U.S. or Canada. The wide scope of online advertisement of smuggling services is reflected not only by the various routes concerned, but also by the variety of nationalities targeted by smugglers. However, most reports indicate that advertisement targets Arab speaking irregular migrants. Numerous reports reveal dedicated groups and channels where communication is in Farsi, or social media pages and apps with Arabic names.

[4] ITV News, 2021- People smugglers to face new maximum life sentence [2 March, 2021] accessible at https://www.itv.com/news/2021-03-01/people-smugglers-to-face-new-maximum-life-sentence-itv-news-understands

Online advertisement included offers for a variety of means of transportation, which together with the volume and complexity of the services traded, directly influence the smuggling fees. Criminals use the online domain to advertise smuggling by sea, in unseaworthy vessels[5], on cargo or commercial ships, in rubber or speedboats, on tourist yachts or other leisure vessels, by air, via commercial flights, by foot, or in vehicles (including cars, heavy goods vehicles or trucks).

Social media is also used to recruit and commission low-level facilitators, particularly drivers. In one case, Instagram services were used to recruit Polish drivers willing to transport Albanian irregular migrants through France, to the UK, for a fee of GBP 8 000 to 10 000.[6] In another case, two Polish truck drivers shared videos of their journeys throughout Europe on a Youtube channel, and described how another Instagram user would send them requests for transporting Albanian irregular migrants.

Investigations have also revealed suspected involvement of companies, including currency exchange offices and travel agencies associated with social media accounts advertising facilitation. Such companies may be used as front businesses by smugglers, to divert law enforcement attention from the true purpose of their activities.

[5] ITV News, 2021 – People smugglers to face new maximum life sentence (2 March, 2021) accessible at https://www.itv.com/news/2021-03-01/people-smugglers-to-face-new-maximum-life-sentence-itv-news-understands

[6] Europol data – AP Migrant Smuggling

Communication and instructions

While the initial contact between smugglers and irregular migrants is established often on social media platforms, further communication is carried out, for security reasons, via secured and encrypted communication applications – FaceTime, IMO, Messenger, Signal, Skype, Viber, WhatsApp, WeChat, Zalo etc. Contact details are posted on advertisement pages and often lead, directly or indirectly, to several other messaging, social media or video-sharing platforms where details are provided and remote facilitation services are delivered.

Criminal business model using digital tools and services

According to Frontex information, a suspect operating from Albania smuggles Pakistani and Bangladeshi migrants by instructing them on where and how to cross the Greek – Albanian border illegally, and by transporting them to Tirana, in Albania, for a price ranging between EUR 150 and 300. The smuggler uses a Facebook profile for communication via the private chat and video call functions of the Messenger application. The smuggler follows a certain timeline during his communications and always requests a live conversation with the camera on, to check whether the migrants are in police custody, and/or involved in a police operation. The smuggler deletes all messages after every conversation with the migrants. The smuggler remotely guides migrants on how to cross the Greek-Albanian border near Kakavija (ALB) and then provides transportation from a pre-defined meeting point. The smuggler uses Facebook Messenger to send the migrants the coordinates of the meeting point and instructions on how to reach it. The coordinates usually point to a plough field or dirt road close to Gjirokaster (ALB) or Grapsh (ALB). Either an unknown driver or the smuggler himself picks up the migrants from the meeting point then takes them to Tirana (ALB). The facilitation fee is paid to the driver or to the smuggler in cash. Information received also indicates that the suspect had difficulties with getting migrants through the border and to move them to Tirana (ALB) due to COVID-19 lockdown measures, and the smuggler requested migrants to postpone their transport until the lockdown is lifted. The smuggler has however become active again and has been involved in the smuggling of Bangladeshi citizens at the beginning of June 2020. 2021 debriefing interviews indicate the smuggler is still active.

Guidance for smuggling on foot or in vehicles is most frequently provided through instant messaging applications. However, facilitation by air was also reported as managed by smugglers similarly, with applications often used for sharing fraudulent documents for travelling. Information, various instructions, satellite images and photos, planned routes, Google Maps waypoints, GPS data or coordinates, locations, guidance via voice and video messages or, in one case, the link to an application enabling irregular migrants to send their location, are shared via WhatsApp or other popular instant messaging solutions.

Social media pages and video sharing platforms like Youtube are also used for providing instructions to irregular migrants in various stages of their journey. In some instances, it cannot be determined whether the posts originate from migrant smugglers or from successful migrants sharing their expertise.

Role of mass video-sharing platforms in migrant smuggling

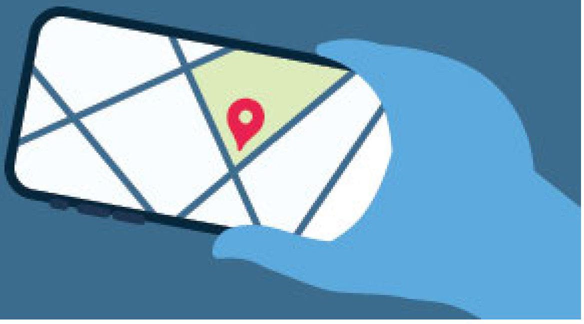
A video was uploaded on a YouTube channel explaining in Arabic-French language how to safely cross the border between Turkey and Greece, near the Bulgarian border. According to the video, a new and safer route from Turkey to Europe for those who want to illegally travel to Europe had been found. Various routes and milestones are shown in the video – through Greece, to the Bulgarian border and from there to the city of Xanthi where, without entering the city, migrants are instructed to reach the train station and travel by train towards Albania, Montenegro, Bosnia and Herzegovina, and Slovenia, before finally reaching Italy.

Furthermore, candidate irregular migrants may be more vulnerable to influencers and peers already in the EU who are documenting every step of their journey on YouTube, potentially reaching hundreds of thousands of viewers and encouraging other young migrants to use the same methods for travelling illegally. The impact could be even greater, if considering that smugglers are advertising their services to potential migrants by posting comments on the videos.[7]

Messaging applications are used for communication between irregular migrants, organisers and drivers. Irregular migrants send the organiser their position and the latter deploys the driver to the location. Such tools were reported on routes through the Western Balkan region, through Poland and further to the United Kingdom, from Slovenia to Italy or from Hungary, close the green border with Croatia, to the Austrian border and further to Germany.

[7] BBC News, 2021, "Are migrant YouTubers influencing others to travel to the EU?" (February, 2021), video accessible at https://www.bbc.co.uk/news/av/world-europe-56132392

Guidance via mapping apps



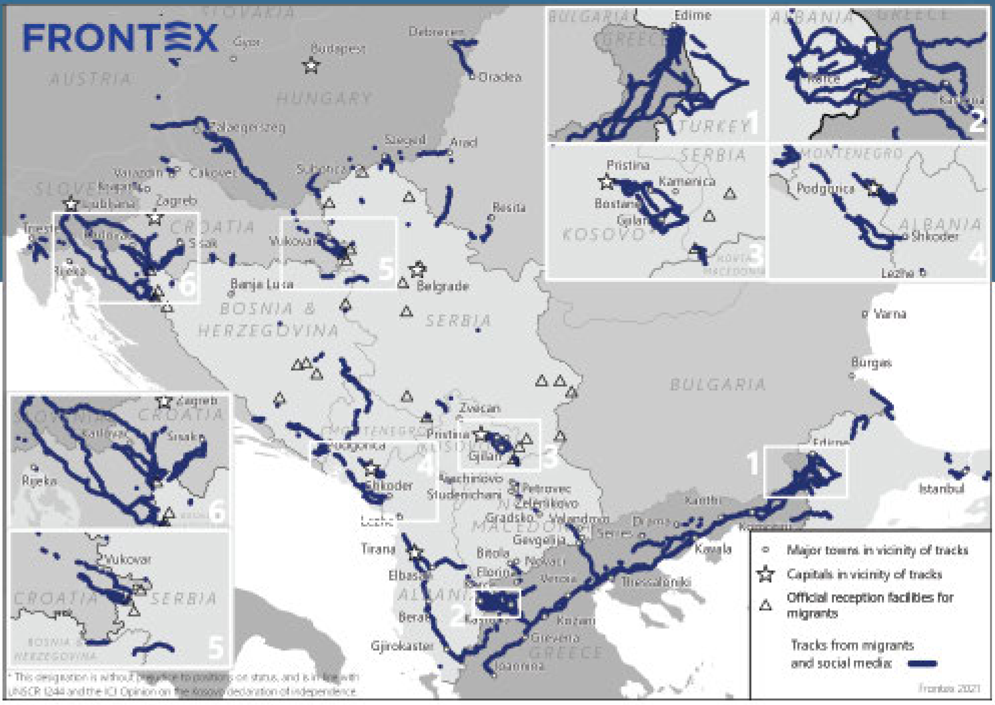
Mapping applications are a key tool used by irregular migrants, either independently or as a part of facilitation services provided by smugglers. Applications such as Maps.me and Google Maps are primary tools[8], often supplemented with readily available online instructions and tutorials on YouTube, and on open or private groups in social media or instant communication platforms. These channels contain detailed guides on how to use the apps and navigate land routes, including where to cross international borders, how to find smuggling hotspots, how to apply for asylum, how to seek shelter and humanitarian assistance, how to get a more powerful smartphone via charity and how to reach refugee camps along the way. Tutorials and chat groups alert migrants about roads and areas to avoid, in very detailed steps illustrated on the mapping applications, giving smugglers a low-risk/high-gain position. Mapping apps are an easy to use tool, allowing irregular migrants not only access to readily available data needed for travelling, but also to create or edit maps and routes within the apps or to share and operate them offline. From smugglers' perspective, such tools provide a risk-free way to capitalize on demand for smuggling services, as they allow criminals to provide their services remotely and to "crowdsource" information on illegal routes by receiving feedback from the migrants. This hypothesis is supported also by the variety of languages used to name the various waypoints found.

Initially, this modus operandi appeared to be particularly used by Northern African irregular migrants, namely Moroccans and Algerians, as an option to travel without relying on smuggling networks and save money. However, Frontex intelligence suggests that the popularity of mapping applications recently increased also among South Asians, in particular Bangladeshi and Pakistani migrants. Similarly, Syrians, Iraqis and, only recently, Afghans reported that they made use of mapping applications at least for one leg of their journey to Europe.

Migrants who opt for this travelling mode are usually single adult males, moving from Turkey to Greece and towards the Western Balkan region, without families. It is also common for migrants who use mapping applications to travel in small groups of people, often made up of co-nationals. In this configuration, normally one of them would receive links to the routes (on Google Maps or Maps.me) via WhatsApp or other messaging apps, from smugglers, relatives in EU MS, friends or fellow migrants who successfully travelled to their desired destination country.

Recent information shows that smugglers try to adapt to the preference of migrants for travelling without facilitation by increasing the attractiveness of their services. In some cases, smugglers offer migrants links to full routes, but also the possibility to

[8] Curry, T., Croitoru, A., Crooks, A. and Stefanidis, A. (2019) 'Exodus 2.0: crowdsourcing geographical and social trails of mass migration', Journal of Geographical Systems, 21(1), 1614, available: https://link.gale.com/apps/doc/A578102433/AONE?u=tou&sid=AONE&xid=24f46dcf [accessed 15 Apr 2021].



* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of independence.

Frontex 2021

Figure Migratory routes uploaded into mapping applications and used by migrants for travelling illegally across the Western Balkan region.

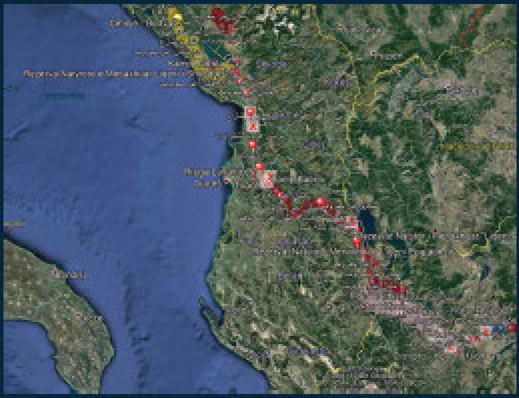
pay for one map describing the route across a specific territory at a time; once the migrant completes the first leg of the journey, they purchase from the same smuggler the map describing the next stage of the illegal crossing. According to Frontex data, migrants reported that they purchased files containing routes generated on the basis of waypoints and placemarks, from smugglers operating in Istanbul, Edirne, Thessaloniki, or Athens, which are considered to be the main migration hubs in the region.

The use of mapping applications has been most popular on smuggling routes via Turkey, Greece and the Western Balkan region. However, during 2020 and 2021, mapping apps used for illegal crossings, both by smugglers and irregular migrants, has spread to routes leading to or crossing other EU MS, such as Poland, Hungary and Romania, or neighbouring countries such as Ukraine and Serbia. With regard to the Western Balkan routes, according to Frontex data, irregular migrants and smugglers may be exploiting a set of long-distance hiking trails in the area, known collectively as the "Via Dinarica", which consists of marked mountain itineraries with huts, shelters and campsites along the way. Such trails are described in detail and can be both downloaded for offline reference and imported into mapping applications. Also, many routes either end or start in the proximity of refugee camps in the Western Balkans region while labelling of waypoints laid at the Albanian borders with Greece reveal that migrants are using the notorious dismissed military bunkers[9] of Enver Hoxha era, as makeshift shelters.

[9] BBC, 2018, "The Cold War bunkers that cover a country" [November 2018] available at https://www.bbc.com/future/article/20181102-the-cold-war-bunkers-that-cover-a-country

Mapping tools in migrant smuggling: Maps.me and Google Maps

Irregular migrants receive geographic indications contained in.KMZ[10] files which they open in Maps.me, an app providing offline maps and navigation, based on geographic data sourced from Open Street Maps. These files can also be opened with Google Earth, to display waypoints and placemarks over rich geographical features. The waypoints deliver a detailed assortment of information – from where to find a charity offering food/shelter/assistance or Wi-Fi hotspots, to which bus to take to reach a city, from where military camps or police stations are located to how to circumvent border crossing points (BCPs). Migrants using the Maps.me application on their smartphones can download maps around the waypoints along the routes of their interest, simply by tapping on any of them, before the start of their journey or anywhere a Wi-Fi connection is available. They can also drop waypoints on the maps and pinpoint their location, then share it via a messaging application with the smugglers, or receive the waypoint from the smuggler and wait to be picked up. They can contribute to the refinement and expansion of the offline routes themselves, and they can select the means of transport to a selected waypoint.



The names of the waypoints are in a variety of languages: Arabic, Farsi, English, French, Turkish, Albanian, Bulgarian, Macedonian, Greek and others and their colour codes seem to have a consistent logic, with, for example light blue indicating railway stations or bus stations, pink indicating seaports, orange for accommodations, charities, mosques, supermarkets, Wi-Fi hotspots, brown for police or military or green for forested areas or agricultural fields. Each waypoint has a range of metadata attributes, such as coordinates, altitude or free text descriptions. However, checking the waypoint properties on Google Earth or Maps.me, or analysing the KML[11] code does not reveal any further note or explanation, contact details or personal data.

Similar to Maps.me, irregular migrants receive links to a set of Google Maps placemarks ("dropped pins") which they can update and amend as they travel. Anyone with a Google account can follow these routes on Google Maps, can share them on Facebook or Twitter and display the nickname of the Google Maps user who created them. Unlike Maps.me, Google Maps requires an internet connection. However, the latter allows the downloading of maps around a chosen position or placemark, for offline use.

[10] KMZ is a compressed version of a KML file. Keyhole Markup Language or KML is a script language like HTML for expressing geographic annotation and visualisation, used for example on Google Maps.

[11] Keyhole Markup Language or KML is a script language like HTML for expressing geographic annotation and visualisation, used for example on Google Maps.

Money transfer

While information on digital tools and online services used for financial transactions is limited, some reports reveal money transfer applications used by facilitated irregular migrants, payments done through Western Union and communication regarding payments, carried out via online messaging services like Facebook Messenger, WhatsApp or Viber. While there is a presumption that most payments for smuggling fees are done physically by the migrants or their family members, often via a hawala agent or directly to the smugglers, digital services may be used to communicate the proof of payment without the need for a physical contact. The modus operandi used by some smugglers occasionally implies provision of concrete smuggling information – real-time or on pre-planned smuggling events, only after the potential client has sent the organiser a proof of payment. This modus operandi was reported in relation to smugglers active on the Western Balkan routes, from Greece to Serbia, from Serbia or Romania to Hungary, Austria or Germany, on foot and in concealments of lorries. In other cases, however, payment is requested by smugglers upon arrival to the destination[12], which generates additional obstacles in identifying smuggling cases in process.

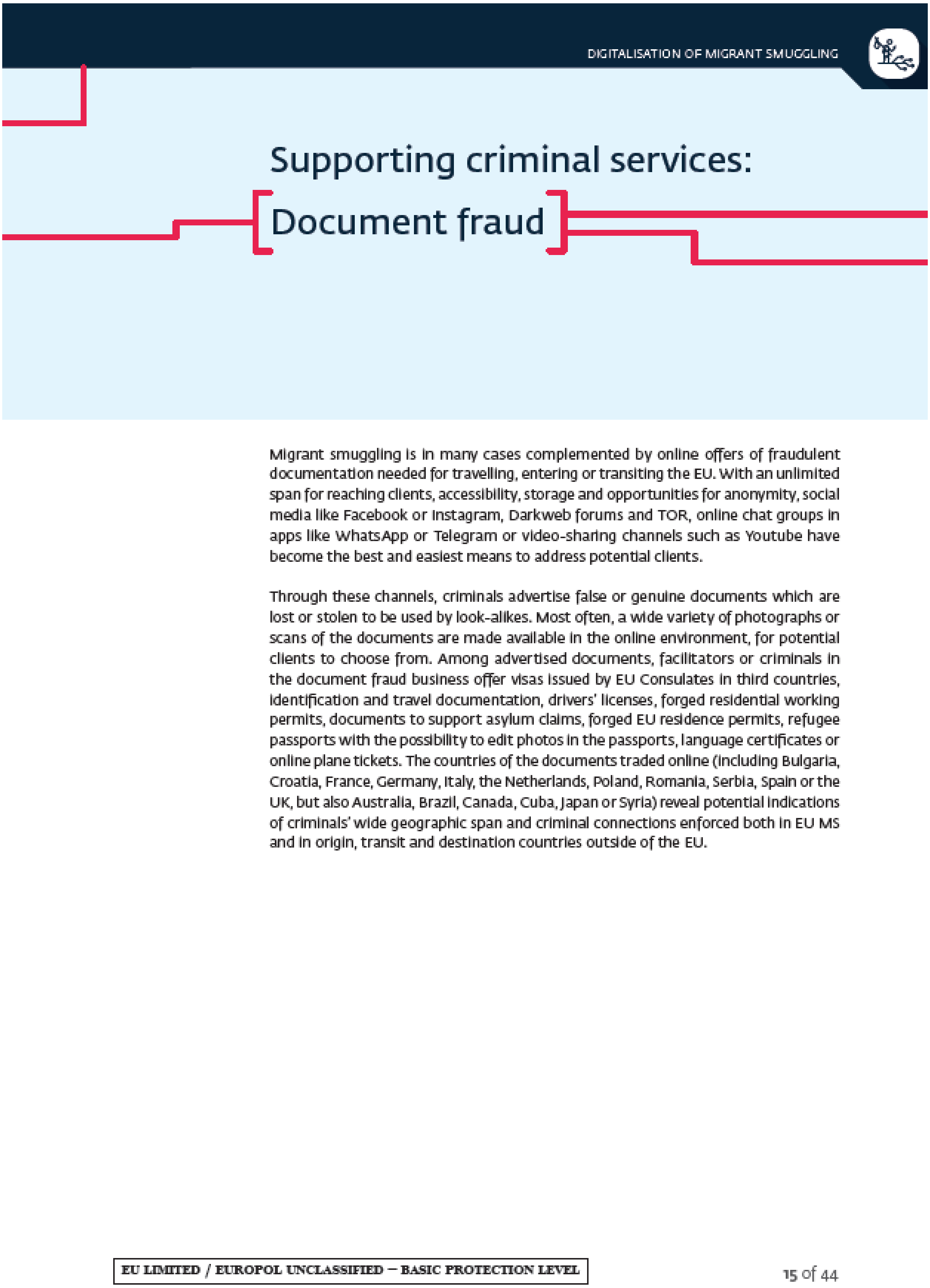
[12] Europol data – AP Phoenix

Countermeasures

In addition to supporting various stages of the migrant smuggling process, digital services are often employed by criminals as countermeasures. Such solutions are used equally by smugglers and by irregular migrants, as instructed or provisioned by smugglers. Among digital solutions used as a countermeasures in the migrant smuggling business, reports reveal software and apps used to:

- Lock, conceal and disguise content on devices (AppLock, Secure Folder), (Knox, Sgallery, FakeChat)
- Erase content (Erase photos) and accounts from devices, recover content (DiscDigger)
- Generate temporary emails, clone apps (Clone App), modify GPS locations (FakeGPS), display caller ID (Numberbook)
- Ensure private internet connection (Hola VPN, Thunder VPN, Psiphon Pro, Hexatech, SuperVPN and LinkVPN).

Burner applications are used to generate temporary phone numbers which irregular migrants and smugglers exploit for their communication or in creating additional social media and instant messaging accounts, with minimal risks of law enforcement monitoring or interception. Such practices pose additional challenges since burner applications are a legally provided service, therefore direct law enforcement measures cannot be taken against the providers of such solutions.



Supporting criminal services: Document fraud

Migrant smuggling is in many cases complemented by online offers of fraudulent documentation needed for travelling, entering or transiting the EU. With an unlimited span for reaching clients, accessibility, storage and opportunities for anonymity, social media like Facebook or Instagram, Darkweb forums and TOR, online chat groups in apps like WhatsApp or Telegram or video-sharing channels such as Youtube have become the best and easiest means to address potential clients.

Through these channels, criminals advertise false or genuine documents which are lost or stolen to be used by look-alikes. Most often, a wide variety of photographs or scans of the documents are made available in the online environment, for potential clients to choose from. Among advertised documents, facilitators or criminals in the document fraud business offer visas issued by EU Consulates in third countries, identification and travel documentation, drivers' licenses, forged residential working permits, documents to support asylum claims, forged EU residence permits, refugee passports with the possibility to edit photos in the passports, language certificates or online plane tickets. The countries of the documents traded online (including Bulgaria, Croatia, France, Germany, Italy, the Netherlands, Poland, Romania, Serbia, Spain or the UK, but also Australia, Brazil, Canada, Cuba, Japan or Syria) reveal potential indications of criminals' wide geographic span and criminal connections enforced both in EU MS and in origin, transit and destination countries outside of the EU.

Digital leads into migrant smuggling

Leads for timely identification of digital services and tools used for migrant smuggling, particularly at the stage of first encounter with facilitators and irregular migrants, are key for deploying effective immediate measures. They may lead to better chances of preserving evidence, associating potentially unrelated individual detections, and probing into the deeper layers of criminal networks, beyond frontmen and low-level facilitators. In complementarity with building law enforcement skills in spotting signs of and tracing facilitation of migrant smuggling in the vast amount of online content, such approach can provide a strong basis for initiating proactive investigations.

Among the indicators of potential criminal activity, information contributed to Europol reveals elements like membership in closed groups where relevant conversations are carried out or where files, maps, travel directions, routes, navigation advice, geographic coordinates, contacts etc. are shared. Active membership in closed instant messaging groups where most communications were deleted, erased contacts and social media accounts, pages and profiles with relevant names stored in contact lists or conversations revealing advice on using distress phone numbers at certain points of the journey or applications containing practical information such as contact information of lawyers, NGOs, shops etc. are additional elements generating suspicions of coordinated illegal activity.

Additionally, files containing photographs of identity and travel documents, routes or maps, videos presenting examples of facilitation, travel directions or locations, are signs of suspected criminal activity, together with special keywords or codes used in dedicated groups or in search histories, or activity history connected to groups and online pages where facilitation services are advertised and promoted.

While most cases reported to Europol refer to the use of digital services and online platforms to advertise illicit activities, to recruit irregular migrants or low-level facilitators, or to organise and guide smuggling, indications of criminal activities may be revealed also by details connected to financial transactions including hawala payment codes and receipts, suspicious payment information or communication, suspicious links to online financial services or bank accounts found in the devices of smugglers or irregular migrants.

In criminal hands, cryptocurrencies deliver significant opportunities for money laundering, anonymity and even profits augmentation. With fees for transferring cryptocurrencies via money-sending platforms significantly lower than those imposed for traditional currency transfer[13], this currency may become more popular in the migrant smuggling milieu. Therefore, in addition to indications of payments in traditional currencies, identification of apps for cryptocurrency transfer, crypto addresses or of other traces of operations with cryptocurrencies, may deliver insight or raise suspicions regarding potential criminal activity.

Numerous reports reveal an increasing interest and use of technical solutions for concealing content in devices, particularly in mobile phones. As such, applications which conceal content under traditional logos in phones or computers, encryption tools for communication and social media content, use of several phone numbers, emails and accounts on one device, apps modifying GPS coordinates, concealing real phone numbers or displaying fictitious numbers to the recipient of messages may be also considered suspicious elements that should instigate additional checks and more in-depth investigations.

[13] For example, the Western Union fee for Africa and Middle East is about EUR 10 to 20 for a EUR 200 transaction, instead of EUR 1 per a cryptocurrency transaction of EUR 10.0000.

Impact of migrant smuggling digitalisation

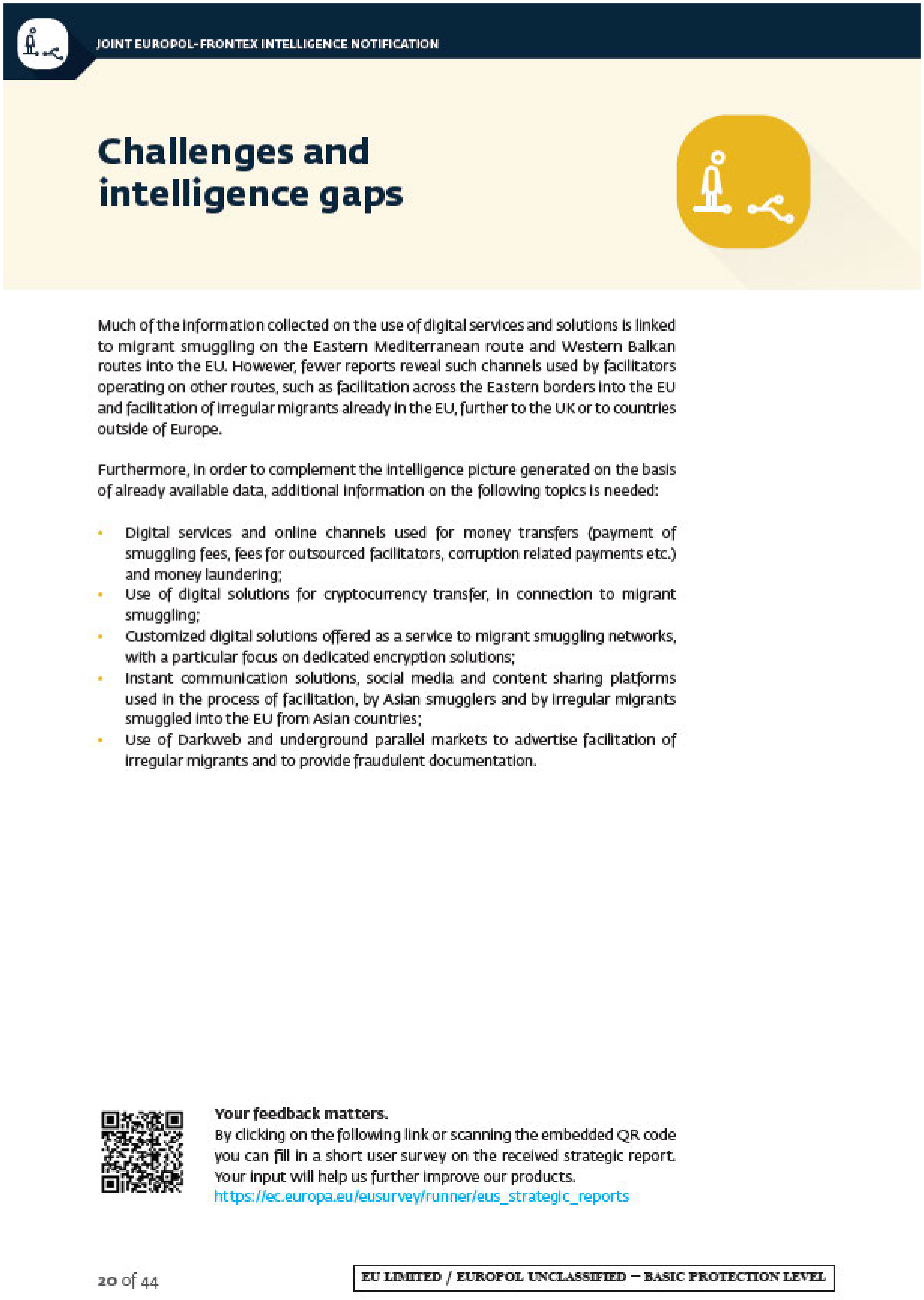
The market for digital products is continuously developing, with providers delivering solutions increasingly tailored to the needs of customers. Over the last years, digital tools have become an organic part of serious and organised crime – including migrant smuggling, and have led to a visibly increased volume of online criminal content. As a result, digitalisation is most likely to continue to penetrate all layers of criminal operations, as it provides a low-risk and low-cost method for criminals to operate undeterred by law enforcement. Digital tools are easily accessible and, in most cases, free of charge, driving both criminals and irregular migrants to naturally resort to the use of apps and online platforms to facilitate illegal travel and border crossings into and through EU MS. Additionally, many instant communication channels provide a secure environment for communication, allowing criminals to successfully shield their involvement from law enforcement.

While also shielding the leadership of criminal networks and allowing them to manage their business remotely, on an operational level, the use of digital apps and opportunities offered by the online environment allows smugglers to limit or altogether exclude direct contact with their clients. With digital tools and mass communication platforms widely available to the large public, smugglers can advertise their services online, share relevant information and instructions, making access to facilitation easily searchable and retrievable. Furthermore, criminals exploit crowdsourced user information, such as the details contributed by irregular migrants to migratory routes in mapping apps, and may benefit from free advertisement from their clients, by means of direct communication and sharing of contacts within their communities, or via video-sharing platforms where they present their experiences.

Digitalisation of criminal activities overall, and of migrant smuggling in particular, opens-up additional opportunities for recruitment, particularly in the most exposed, lower levels of the networks, where facilitation occasionally takes the form of ad-hoc services. As a result, a large pool of collaborators are attracted into criminal activities for a fee, without necessarily forming part of smuggling networks, adding yet another layer of protection for network leadership and for the organisers.

Following the successful example of document fraud, development of digitalisation as a service poses additional challenges for law enforcement. As seen in other crime areas, experts in developing digital solutions for the use of criminals may become more active on the markets for migrant smuggling. As such, a parallel supporting business may develop, independently servicing criminal clients, providing customised digital solutions for encrypted communications, travel guidance, payment of smuggling fees or provision of fraudulent documents. Information indicates a limited use of the Darkweb and cryptocurrencies in connection to migrant smuggling. However, with the rapid development and volatility of digital markets, against the background of an increasing need for safe, cheap and fast communication from criminals, the emergence of such tools and channels must not be disregarded by law enforcement.

The online environment and the wide array of easily accessible digital solutions increase the efficiency and professionalisation of migrant smugglers, allowing them to become more agile and resilient against intervention from law enforcement, and to maintain a minimal direct implication in criminal operations. In such a dynamic environment, law enforcement must demonstrate not only its investigative skills, but also proactivity in integrating innovative techniques in the fight against migrant smuggling and in identifying digital traces of such criminal activities.



Challenges and intelligence gaps

Much of the information collected on the use of digital services and solutions is linked to migrant smuggling on the Eastern Mediterranean route and Western Balkan routes into the EU. However, fewer reports reveal such channels used by facilitators operating on other routes, such as facilitation across the Eastern borders into the EU and facilitation of irregular migrants already in the EU, further to the UK or to countries outside of Europe.

Furthermore, in order to complement the intelligence picture generated on the basis of already available data, additional information on the following topics is needed:

- Digital services and online channels used for money transfers (payment of smuggling fees, fees for outsourced facilitators, corruption related payments etc.) and money laundering;
- Use of digital solutions for cryptocurrency transfer, in connection to migrant smuggling;
- Customized digital solutions offered as a service to migrant smuggling networks, with a particular focus on dedicated encryption solutions;
- Instant communication solutions, social media and content sharing platforms used in the process of facilitation, by Asian smugglers and by irregular migrants smuggled into the EU from Asian countries;
- Use of Darkweb and underground parallel markets to advertise facilitation of irregular migrants and to provide fraudulent documentation.

Your feedback matters.
By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report. Your input will help us further improve our products.
https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Annex I: Overview of applications and platforms identified in connection to migrant smuggling

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL

Background

As a result of the analysis carried out for the purpose of the joint Europol-Frontex Intelligence Notification of digitalisation of migrant smuggling, several solutions and platforms have been identified as tools used to facilitate criminal activities, and have been further researched. For each app and platform used in connection to migrant smuggling, this Annex contains links to law enforcement guidelines available under the SIRIUS project hosted by the European Platform for Experts, and general descriptions of the solutions, main functionalities and contact details available in open sources. In complementarity with the outcomes highlighted in the intelligence notification and the content of Annex 2 containing expert recommendations on handling seized mobile communication devices, the aim of this overview is to provide relevant law enforcement agencies in the EU and in Western Balkan countries with information on the solutions used by migrant smugglers and facilitated irregular migrants, in order to enrich opportunities for timely identification of potential indications of migrant smuggling upon contact with suspicious activity, and to direct further investigations on the basis of online criminal content.

SIRIUS – Europol Platform for Experts

The SIRIUS project helps investigators to cope with the complexity and volume of information in a rapidly changing online environment, by providing guidelines and tools, and by sharing experience with peers, both online and in person. SIRIUS is an important reference point, enabling practitioners to develop their knowledge when obtaining electronic data from online service providers (OSPs). Created by Europol in October 2017, the SIRIUS project is a central reference point in the European Union for knowledge sharing on digital cross-border investigations for law enforcement and judicial authorities. SIRIUS products and services are currently available to all EU Member States and 17 non-EU countries.[14]

[14] For more information, visit www.europol.europa.eu/sirius, www.eurojust.europa.eu/states-and-partners/eu-partners/europol/sirius-project or contact us for membership as law enforcement official.

Overview of apps and platforms identified in connection to migrant smuggling

Azar

BASIC INFORMATION

Azar is a social networking video chat app that allows instant connection between users around the world. The app is available only on the App Store for iPhone and iPad.

CONTACT INFORMATION

Hyperconnect Inc.
Post 20F, ASEM Tower, 517 Yeongdong-daero, Gangnam-gu
Seoul, Republic of Korea

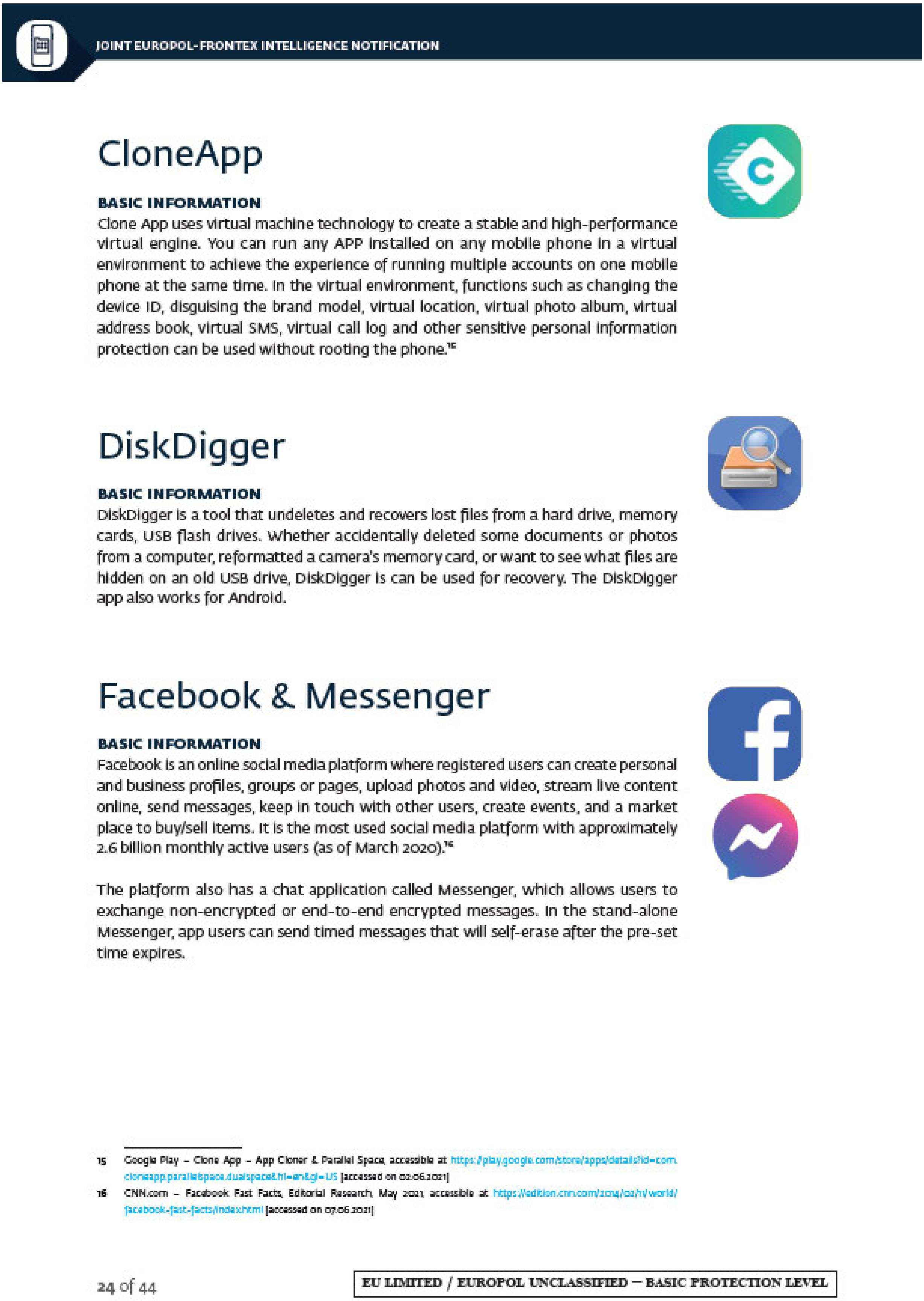
EU Representative
Bird & Bird GDPR Representative Ireland
29 Earlsfort Terrace, Dublin 2, D02 AY28
Ireland

LAW ENFORCEMENT INFORMATION

AZAR transfers or discloses personal information to Government authorities, judicial authorities, regulators or other third parties where required:

They will disclose personal information to government authorities, judicial authorities, regulators or other third parties where they have a legal requirement to do so or where they believe this is necessary:

- to comply with the law or respond to compulsory legal processes (such as a search warrant, subpoena or court order);
- to verify or enforce compliance with the terms and policies governing their Service and to investigate fraud or other unlawful activity relating to the use of the Service or affecting their business, to the extent such disclosure is permitted by applicable data protection laws; and to protect and defend rights, property, and the security or safety of business operations and those of any of their respective affiliates, staff, business partners, customers or members of the public.



CloneApp

BASIC INFORMATION

Clone App uses virtual machine technology to create a stable and high-performance virtual engine. You can run any APP installed on any mobile phone in a virtual environment to achieve the experience of running multiple accounts on one mobile phone at the same time. In the virtual environment, functions such as changing the device ID, disguising the brand model, virtual location, virtual photo album, virtual address book, virtual SMS, virtual call log and other sensitive personal information protection can be used without rooting the phone.[15]

DiskDigger

BASIC INFORMATION

DiskDigger is a tool that undeletes and recovers lost files from a hard drive, memory cards, USB flash drives. Whether accidentally deleted some documents or photos from a computer, reformatted a camera's memory card, or want to see what files are hidden on an old USB drive, DiskDigger is can be used for recovery. The DiskDigger app also works for Android.

Facebook & Messenger

BASIC INFORMATION

Facebook is an online social media platform where registered users can create personal and business profiles, groups or pages, upload photos and video, stream live content online, send messages, keep in touch with other users, create events, and a market place to buy/sell items. It is the most used social media platform with approximately 2.6 billion monthly active users (as of March 2020).[16]

The platform also has a chat application called Messenger, which allows users to exchange non-encrypted or end-to-end encrypted messages. In the stand-alone Messenger, app users can send timed messages that will self-erase after the pre-set time expires.

[15] Google Play – Clone App – App Cloner & Parallel Space, accessible at https://play.google.com/store/apps/details?id=com.cloneapp.parallelspace.dualspace&hl=en&gl=US [accessed on 02.06.2021]

[16] CNN.com – Facebook Fast Facts, Editorial Research, May 2021, accessible at https://edition.cnn.com/2014/02/11/world/facebook-fast-facts/index.html [accessed on 07.06.2021]

CONTACT INFORMATION

For Facebook, different legal entities are considered to be data controllers for various countries/regions:

For EU citizens/residents:
Facebook Ireland Ltd. Attn: Law Enforcement Response Team 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland

For US citizens/residents:
Facebook Inc. 1601 Willow Road, Menlo Park California 94025, United States of America

LAW ENFORCEMENT INFORMATION

Law Enforcement Online Requests System: http://www.facebook.com/records

E-mail for enquiries or requests which cannot be submitted via the portal: records@records.facebook.com

Guidelines for law enforcement are available at: www.facebook.com/safety/groups/law/guidelines.

FaceTime

BASIC INFORMATION

FaceTime is a proprietary video telephony product developed by Apple Inc. FaceTime is available on supported iOS mobile devices running iOS 4 and later and Mac computers that run Mac OS X 10.6.6 and later. FaceTime supports any iOS device and any Mac with a forward-facing camera. FaceTime Audio, an audio-only version, is available on any iOS device that supports iOS 7 or newer, and any Mac with a forward-facing camera running Mac OS X 10.9.2 and later. FaceTime is included for free in iOS and in macOS from Mac OS X Lion (10.7) onwards.[17].

CONTACT INFORMATION

Apple United States:
Apple Inc.,
One Apple Park Way, Cupertino, CA 95014
United States of America

Apple Ireland:
Apple Distribution International
Hollyhill Industrial Estate
Hollyhill, Cork, Ireland

[17] Search Mobile Computing – FaceTime, accessible at https://searchmobilecomputing.techtarget.com/definition/FaceTime [accessed on 09.06.2021]

LAW ENFORCEMENT INFORMATION [18]

Law Enforcement Response Team:
(receives voluntary requests and general inquiry from law enforcement)

Government & Law Enforcement Information Request' template:
https://www.apple.com/legal/privacy/gle-inforequest.pdf

E-mail: lawenforcement@apple.com

For emergencies:
'EMERGENCY – Government & Law Enforcement Information Request' template:
https://www.apple.com/legal/privacy/leemergencyrequest.pdf

E-mail: exigent@apple.com

Google Maps

BASIC INFORMATION

Google Maps is a web mapping and navigation application for desktop and mobile devices from Google. Maps provides turn-by-turn directions to a destination along with 2D and 3D satellite views, as well as public transit information. Maps also offers "Street Views," which are photos of the actual streets and surroundings. Millions of websites use Google Maps for directions to stores and offices. [19]

Hexatech

BASIC INFORMATION

Hexatech is a free VPN proxy application that hides the IP of the user by creating a new IP to essentially mask the existing location[20]. VPN sessions are not logged. Betternet LLC a U.S. company is responsible for Betternet and Hexatech[21]. Data can be shared with LEA based on legal requests but will be limited to what is legal necessary.

[18] Apple.com, Privacy – Government Information Requests, accessible at https://www.apple.com/privacy/government-information-requests/ [accessed on 01.06.2021]

[19] PC Mag, Google Maps, accessible at https://www.pcmag.com/encyclopedia/term/google-maps [accessed on 09.06.2021]

[20] Google Play – VPN by Ultra VPN – Secure Proxy & Unlimited VPN, accessible at https://play.google.com/store/apps/details?id=tech.hexa&hl=en_US&gl=US [accessed on 02.06.2021]

[21] Aura.com – Privacy Policy, accessible at https://aura.com/legal/privacy-policy [accessed on 02.06.2021]

Hola

BASIC INFORMATION

Hola is a VPN mobile application that uses peer-to-peer caching. Besides various worldwide locations, their HQ is situated in Israel[22]. The application is free but premium members can redirect request to peers and are never uses as peers themselves. Like other VPN applications Hola allows anonymous web browsing and circumvents blocked domains. Regarding the privacy policy Hola claims to have no logs for Premium or Ultra subscribers. Furthermore, no logs of traffic incoming and outgoing IP addresses, browsing history session duration etc. are made. Personal information can be exchanged if it complies with law, legislation or following a subpoena or court order[23].

HOLA additionally provides an application for changing your GPS location to wherever you want in the world[24]. This equally affects all other applications on the specific mobile device.

ICQ

BASIC INFORMATION

ICQ New is a cross-platform messenger and VoIP client. The name ICQ derives from the English phrase "I Seek You". Originally developed by the Israeli company Mirabilis in 1996, the client was bought by AOL in 1998, and then by Mail.Ru Group in 2010[25].

The ICQ client application and service were initially released in November 1996, freely available to download. ICQ was among the first stand-alone instant messenger (IM) – while real-time chat was not in itself new (Internet Relay Chat (IRC) being the most common platform at the time), the concept of a fully centralized service with individual user accounts focused on one-on-one conversations set the blueprint for later instant messaging services like AIM, and its influence is seen in modern social media applications. ICQ became the first widely adopted IM platform.

During the second week of January 2021, ICQ saw a renewed increase in popularity in Hong Kong, spurred on by the controversy over WhatsApp's privacy policy update. The number of downloads for the application increased 35-fold there.[26]

[22] Hola (VPN) accessible at https://hola.org/faqein_cost [accessed on 03.06.21]

[23] Hola.org – Hola Privacy Policy, accessible at https://hola.org/legal/privacy [accessed on 03.06.2021]

[24] Hola.org – Hola change GPS location, accessible at https://hola.org/gps [accessed 04.06.2021]

[25] Techspot – What ever happened to ICQ?, accessible at https://www.techspot.com/article/1771- icq/ [accessed on 09.06.2021]

[26] Olhar Digital – With new rules on Whatsapp ICQ wins unprecedented demand, accessible at https://olhardigital.com.br/en/2021/01/26/noticias/com-novas-regras- no-whatsapp-icq-ganha- procura-inedita/?gfetch=2021%2F01%2F26%2Fnews%2Fwith-new-rules-on-whatsapp-icq-wins-unprecedented-demand%2F [accessed on 09.06.2021]

CONTACT INFORMATION

Mail.Ru LLC is located at 39 Leningradsky Pr., Bldg. 79, Moscow, 125167, Russian Federation. They are represented, for the purposes of the privacy policy, by MGL MY.COM (CYPRUS) LIMITED of 28 Oktovriou, 365 VASHIOTIS SEAFRONT, office 402 Neapoli, 3107, Limassol, Cyprus

Law Enforcement Online Request System: https://www.whatsapp.com/records/login

E-mail address for general inquiries from law enforcement: records@records.whatsapp.com

LAW ENFORCEMENT INFORMATION

Russian national legislation[27] does not allow the disclosure of data held by private companies based in the country directly to foreign authorities. This also applies to emergency circumstances.

Encryption of services: Under Russian national legislation, OSPs are obliged to provide the state security agency with decryption information for electronic messages[28].

For additional information, please see the privacy policy.

Cooperation with Russian intelligence services

According to a Novaya Gazeta article published in May 2018, Russian intelligence agencies have access to online reading of ICQ users' correspondence. The article examined 34 sentences of Russian courts, during the investigation of which the evidence of the defendants' guilt was obtained by accessing correspondence on PCs or mobile devices. Of the fourteen cases in which ICQ was involved, in six cases the capturing of information occurred before the seizure of the device[29].

IMO

BASIC INFORMATION

IMO is a free audio/video calling and instant messaging software service. It allows sending music, video, PDFs and other files, along with various free stickers. It supports encrypted group video and voice calls with up to 20 participants. According to its developer, the service possesses over 200 million users and over 50 million messages per day are sent through it.[30]

Within its terms of service IMO included a headline on Reporting Violations and state that they report any activity that they suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties, and may cooperate with such authorities as they may request.

[27] Constitution of the Russian Federation, Federal Law of 27.07.2006 № 152-ФЗ, Directive of the President of the Russian Federation of 22.03.2008№144-pnandFederal Law of 12.08.1995 г. № 144-ФЗ as amended on 06.07.2016, accessible at https://pd.rkn.gov.ru/authority/p146/p164/

[28] The Moscow Times, October 2016, Russia Begins Search for Decryption of Online Messengers, accessible at https://www.themoscowtimes.com/2016/10/04/russia-begins-search-for-decryption-of-online-messengers-55585 [accessed 07.06.2021]

[29] Novaya Gazeta – ICQ and comrade Major, accessible at https://novayagazeta.ru/articles/2018/05/17/76500-aska-i-tovarisch-mayor [accessed on 09.06.2021]

[30] Technobuffalo – IMO Messenger app of the week, accessible at https://www.technobuffalo.com/imo-messenger-app-of-the-week [accessed on 09.06.2021]

CONTACT INFORMATION

IMO is hosted by PageBites Inc.
555 Bryant Street Suite 819
Palo Alto, California 94301, USA

Phone: 01 650-248-6031
mailto: ads@imo.im
Please, also refer to the imo terms of service and privacy policy

Instagram

BASIC INFORMATION[31]

Instagram is a social networking app made for sharing photos and videos; since April 2012 is part of Facebook. Instagram is available for free on iOS, Android and Windows Phone devices. It can also be accessed on the web from a computer yet with limitation: e.g. the messaging functionality is available but photos or videos (except IGTV videos) can only be uploaded and shared from mobile devices.

Instagram does not require e-mail or phone verification, and does not require people to use real names or identities.

User IDs can be found using free online tools like https://findmyfbid.in/findinstagram-id/ or https://codeofaninja.com/tools/find-instagramuser-id

CAVEAT: bear in mind that online services used to locate Instagram's user ID may store searches. Therefore, operational data may be exposed. One search can provide multiple hits, so follow up is required.

CONTACT INFORMATION

As Instagram is part of Facebook there are different legal entities considered to be data controllers for different countries/regions:

For EU citizens/residents:
Facebook Ireland Ltd. Attn: Law Enforcement Response Team 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland

For US citizens/residents:
Facebook Inc. 1601 Willow Road, Menlo Park California 94025, United States of America

Please refer to this publication when considering to submit a data request to Signal: https://signal.org/bigbrother/central-california-grand-jury/

LAW ENFORCEMENT INFORMATION

Law Enforcement Online Requests System: http://www.facebook.com/records

E-mail for enquiries or requests which cannot be submitted via the portal: records@records.facebook.com

[31] Excerpt cited from the SIRIUS Europol Platform for Experts

KNOX

BASIC INFORMATION

Samsung Knox is a proprietary security framework pre-installed on most Samsung mobile devices. Its primary purpose is to provide organizations with a toolset for managing work devices, such as employee mobile phones or interactive kiosks. Knox provides more granular control over the standard work profile to manage capabilities found only on Samsung devices.

Knox's features fall within three categories: data security, device manageability, and VPN capability. Knox also provides web-based services for organizations to manage their devices. Organizations can customize their managed mobile devices by configuring various functions, including pre-loaded applications, settings, boot-up animations, home screens, and lock screens.

As of December 2020, organizations can use specific Samsung mobile device cameras as barcode scanners, using Knox services to capture and analyze the data.

A test version for iOS is available as well for iPhone and iPad. It is intended to provide complete and full Knox feature support over time. The developer, SAMSUNG SDS Co.,LTD., indicated that the app's privacy practices may include handling of data as described above. For more information, see the developer's privacy policy[31].

LinkVPN

BASIC INFORMATION[33]

LinkVPN is similar to the previous mentioned VPNs. It is free to use and hides the users IP whilst encrypting internet websites without saving logs. FuryWeb Tech. offers the App. The Company is situated in Hong Kong[34]. Personal information about the customer will not be shared except with other service providers (e.g. distributers, resellers and app store partners).

[32] Samsung Knox, Manage Samsung Knox devices with MDM, accessible at https://www.manageengine.com/mobile-device-management/samsung-knox-management.html [accessed on 09.06.2021]

[33] Uptodown.com -LinkVPN accessible at https://linkvpn.en.uptodown.com/android [accessed on 03.06.2021]

[34] Policy privacy accessible at http://139.162.156.236/assets/privacy.html [accessed on 03.06.2021]

Maps.me

BASIC INFORMATION [35]

Maps.me (styled as MAPS.ME) is a mobile app for Android, iOS and BlackBerry that provides offline maps using OpenStreetMap data. It was formerly known as MapsWithMe. In November 2014, it was acquired by Mail.Ru Group and became part of its My.com brand.

On 2 November 2020, Mail.ru Group Limited announced the sale of MAPS.ME to Daegu Limited (member of Parity.com Group).

For additional information, please refer to the Privacy policy and the terms of service.

Numberbouk

BASIC INFORMATION [36]

Numberbouk is a phone, e-mail and mobile number directory that allows its users to search by mobile number, name, as well as an e-mail.

You can find the privacy policy here.

Odnoklassniki

BASIC INFORMATION

Odnoklassniki (Russian: Однокла́ссники, English: Classmates) is a social network service used mainly in Russia and former Soviet Republics

The website currently has more than 200 million registered users[37] and 45 million daily unique visitors. Odnoklassniki also currently has an Alexa Internet traffic ranking of 56 worldwide and 7 for Russia. Odnoklassniki is the second most popular social network in Russia, behind VK (VKontakte) but ahead of Facebook, which is in 3rd place[38].

Odnoklassniki is owned by Mail.ru Group with URL www.Odnoklassniki.ru or short www.ok.ru whereas domains of the mobile version of Odnoklassniki have the prefix m. (m.ok.ru).

("OK" or OK.ru) is the oldest Russian social network. The site was launched in March 2006, seven months ahead of the other primary social network in Russia, Vkontakte

[35] PanoramaCrypto– Maps.me, accessible at https://panoramacrypto.com/maps-me-is-a-navigation-app-that-will-have-a-crypto-wallet-and-defi/ [accessed on 09.06.2021]

[36] Numberbouk.com, accessible at http://www.numberbouk.com/About [accessed on 03.06.2021]

[37] Dreamgrow.com – Social Media in Russia, accessible at https://www.dreamgrow.com/social-media-in-russia/ [accessed on 09.06.2021]

[38] Archive.today – Odnoklassniki.ru – accessible at https://archive.is/20120118002705/http://odnoklassniki.ru/cdk/st.cmd/helpAbout/tkn/729 [accessed on 02.06.2021]

("VK"). Both sites are owned by Mail.ru Group, a Russian internet company, which operates internationally under the brand My.com.

My.com is an international subsidiary of Mail.Ru company that offers games and Internet-related services and products. My.com is working under brands and services myMail, myChat, myGames and Maps.Me. My.com is headquartered in Amsterdam, Netherlands, with a U.S. office located in Mountain View, California. Wikipedia

CONTACT INFORMATION

Mail.Ru LLC is located at 39 Leningradsky Pr., Bldg. 79, Moscow, 125167, Russian Federation.

They are represented, for the purposes of the privacy policy, by MGL MY.COM (CYPRUS) LIMITED of 28 Oktovriou, 365 VASHIOTIS SEAFRONT, office 402 Neapoli, 3107, Limassol, Cyprus

LAW ENFORCEMENT INFORMATION

Russian national legislation[39] does not allow the disclosure of data held by private companies based in the country directly to foreign authorities. This also applies to emergency circumstances.

Encryption of services: Under Russian national legislation, OSPs are obliged to provide the state security agency with decryption information for electronic messages[40].Please refer as well to the privacy policy.

Psiphon Pro

BASIC INFORMATION

Psiphon Pro is a free and open source VPN. It was developed by Citizen Lab at the University of Toronto, Canada[41]. Psiphon does not share any personalized data with third parties.[42]

Secure Folder

BASIC INFORMATION

Secure Folder by Samsung is an encrypted space on smartphones to store files, images, videos, and apps. The service keeps all sensitive files private. Originally launched as part of Samsung Knox, Samsung Secure Folder comes pre-installed on many of Samsung's smartphones[43].

[39] Constitution of the Russian Federation, Federal Law of 27.07.2006 № 152-ФЗ, Directive of the President of the Russian Federation of 22.03.2006№144-prandFederal Law of 12.08.1995 г. № 144-ФЗ as amended on 06.07.2016 – accessible at https://pd.rkn.gov.ru/authority/p146/p164/

[40] The Moscow Times, October 2016, Russia Begins Search for Decryption of Online Messengers, accessible at https://www.themoscowtimes.com/2016/10/04/russia-begins-search-for-decryption-of-online-messengers-a55585 [accessed 07.06.2021]

[41] Psiphon.ca – Psiphon – a technical desciption, accessible at https://psiphon.ca/en/blog/psiphon-a-technical-description [accessed on 09.06.2021]

[42] Psiphon.ca – Privacy policy, accessible at https://psiphon.ca/en/privacy.html [accessed on 03.06.2021]

[43] Samsung – What is the Secure folder and how to use it, accessible at https://www.samsung.com/uk/support/mobile-devices/what-is-the-secure-folder-and-how-do-i-use-it/ [accessed on 09.06.2021]

Sgallery

BASIC INFORMATION

Sgallery is a privacy protection app for Android to easily hide and encrypt photos, videos, apps and any other files for additional privacy.

Sgallery can hide its app icon and keep privacy safe. One can import private images and videos in this secure space. The application can be disguised as a calculator or a system converter[44].

Signal

BASIC INFORMATION

Signal is an encrypted communications application that uses the internet to send one-to-one messages, voice notes, files, images, videos and can make one-to-one calls and video calls.

Signal is end-to-end encrypted by default, the broad set of personal information that is typically easy to retrieve in other apps simply doesn't exist on Signal's servers[45].

CONTACT INFORMATION

Signal Messenger, LLC
Attn: Privacy Signal Messenger, LLC
650 Castro Street, Suite 120-223, Mountain View, CA 94041, USA

LAW ENFORCEMENT INFORMATION

According to the company last statement, the only information they host is the time of account creation and the time of account´s last connection to Signal servers.

The Signal Terms & Privacy Policy can be accessed here.

Please refer to this publication when considering to submit a data disclosure request to Signal:
https://signal.org/bigbrother/central-california-grand-jury/.

[44] Google Play Sgallery – Hide photos, hide videos, gallery vault, accessible at https://play.google.com/store/apps/details?id=com.hid.anzenbokusui&hl=en&gl=US [accessed 03.06.2021]

[45] WebArchive.org – Internetsociety.org – When Signal hits the fan, accessible at https://web.archive.org/web/20160828135326/https://www.internetsociety.org/sites/default/files/09%20when-signal-hits-the-fan-on-the-usability-and-security-of-state-of-the-art-secure-mobile-messaging.pdf [accessed on 09.06.2021]

Skype[46]

BASIC INFORMATION

Skype is a Microsoft instant messaging application best known for its online text message and audio/video chat services. The service is free, but services like Skype Credit or a subscription can be also purchased.

Additionally Skype offers the opportunity to share files, create polls and transfer money. A Skype Number is a second phone number attached directly to the Skype account, allowing the user to answer incoming calls on the Skype app anywhere. People can call the user from their mobile or landline and the call is picked up in Skype.

CONTACT INFORMATION

Contact Information

For EU-based requests (with addition of Iceland, Liechtenstein, Norway, United Kingdom and Switzerland):
Microsoft Ireland Operations Limited ("MIOL"),
One Microsoft Place, South County Business Park, Leopardstown,
Dublin 18, D18 P521, Ireland

Law Enforcement Response Team:
Microsoft has local contacts in different countries. Contact the company via e-mail to request a point of contact in your country: globalcc@microsoft.com

Emergencies (defined by Microsoft as "danger of death or serious physical injury to a person"): LEALERT@microsoft.com

LAW ENFORCEMENT INFORMATION

Law Enforcement Response Portal:
Microsoft has initiated the roll out of their portal in some EU Member States. Get in touch with the company's point of contact in your country for more information.

Microsoft does not have guidelines for authorities that are publicly available, though they may be requested via e-mail to: msnwwcc@microsoft.com

SuperVPN

BASIC INFORMATION

SuperVPN is a free VPN proxy offered by SuperSoftTech, a company situated in Singapore. In accordance with the privacy policy,[47] personal data will not be shared except for analytical or diagnostic matters among other service providers.

[46] Excerpt cited from the SIRIUS Europol Platform for Experts

[47] SuperVPN Privacy Policy, accessible at https://www.supervpn.best/privacy.html [accessed on 03.06.2021]

Telegram[48]

BASIC INFORMATION

Telegram is a cloud-based mobile, tablet and desktop instant Messaging app to exchange text, photos, videos, voice and video calls, stickers and files of any type and size. It is similar to messaging apps like WhatsApp and Facebook Messenger in terms of user experience. The app allows the user to create also secret chats with full end-to-end encryption and even set messages and content to self-destruct after a specific amount of time. It can also be used on different devices at the same time with seamless sync. The company is known to have moved its offices several times between different jurisdictions: according to the platform website, the Telegram development team is currently based in Dubai. At the time of writing, Telegram has set up a legal entity that acts as data controller responsible for processing of data of users based in the European Economic Area: Telegram UK Holdings Ltd (71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ).

CONTACT INFORMATION

The contact details provided by Telegram officially is the e-mail address: abuse@telegram.org which should be used to report content that violates their terms and conditions (see dedicated section).

LAW ENFORCEMENT INFORMATION

Although Telegram has been responsive to law enforcement requests for take down of terrorist related content on some occasions, at the time of writing, the company states that they have never replied to data-disclosure requests. They also do not have publicly available guidelines for authorities. The only information available on requests by law enforcement authorities is available on: https://telegram.org/privacy and states that if Telegram "receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities".

Thunder VPN

BASIC INFORMATION

Thunder VPN, offered by Signal Lab situated in US Alabama, is a VPN proxy that offers internet privacy like the above mentioned VPN for free[49]. Within the privacy policy sharing data with law enforcement or other agencies is not mentioned per se[50].

[48] Excerpt cited from the SIRIUS Europol Platform for Experts

[49] Google Play – Thunder VPN, accessible at https://play.google.com/store/apps/details?id=com.fast.free.unblock.thunder.vpn&hl=en&gl=US, [accessed on 03.06.2021]

[50] Thunder.free-signal.com – Terms of Service, accessible at https://thunder.free-signal.com/Terms%20of%20Service.html, [accessed 03.06.2021]

TikTok

BASIC INFORMATION

TikTok is a social media application owned by ByteDance and available in most countries except China. The app, available for both Android and iOS users, focuses on short videos (Public or Private ones) of 3 to 15 seconds or looping ones up to 1 minute[51].

CONTACT INFORMATION

Different legal entities are considered to be data controllers for different countries/regions:

For residents in the European Economic Area and Switzerland:
TikTok Technology Limited
10 Earlsfort Terrace, Dublin, D02 T380, Ireland

For residents in the United Kingdom:
TikTok Information Technologies UK Limited
6th Floor, One London Wall, London, EC2Y 5EB
United Kingdom

For residents in the United States:
TikTok Inc.
5800 Bristol Parkway, Suite 100, Culver City, CA 90230
United States of America

For residents in countries other than those listed above:
TikTok Pte. Ltd.
1 Raffles Quay, #19-11, South Tower, Singapore 048583

LAW ENFORCEMENT INFORMATION

Guidelines for law enforcement are available on the company's public website:
https://www.tiktok.com/legal/law-enforcement?lang=en

Law Enforcement Response Team: lert@tiktok.com

TikTok Emergency Disclosure Request Form: https://www.tiktok.com/legal/report/EDR

[51] Slate.com – tiktok app musically guide accessible at https://slate.com/technology/2018/09/tiktok-app-musically-guide.html [accessed on 03.06.2021]

Tor

BASIC INFORMATION

Tor is free and open-source software for enabling anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than seven thousand relays, for concealing a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace the Internet activity to the user. This includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored[52].

Onion routing is implemented by encryption in the application layer of the communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address.

As TOR is no ISP in a default definition, there are no terms of service or privacy policy available.

Twitter

BASIC INFORMATION [53]

Twitter is an online communication platform and networking service used to publish 'tweets': a 280- characters long text that can include photos, videos, GIFs or links. It is possible to see publicly available tweets without having an account on the platform, but in order to post it is necessary to create an account using an e-mail address or a phone number. An e-mail or a SMS text will be sent to verify and confirm the new account.

E-mail addresses can only be associated with one Twitter account at a time and are not publicly visible to others on Twitter.

CONTACT INFORMATION

Different legal entities are considered to be data controllers for different countries/ regions:

For residents in the European Economic Area:
Twitter International Company c/o Trust & Safety – Legal Policy One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland

[52] TOR project, accessible at https://www.torproject.org/about/history/ [accessed on 09.06.2021]
[53] Excerpt cited from the SIRIUS Europol Platform for Experts

For residents outside the European Economic Area (United States/rest of the World):
Twitter, Inc. c/o Trust & Safety – Legal Policy 1355 Market Street, Suite 900 San Francisco, California 94103 United States of America

Legal Request Submissions site: https://legalrequests.twitter.com

Law enforcement response online form (only if you experience issues with Legal Request Submissions site): https://help.twitter.com/forms/lawenforcement

LAW ENFORCEMENT INFORMATION

Guidelines for authorities are available on the company's public website (you can change the language on the bottom-right corner on the webpage) at: https://help.twitter.com/en/rules-andpolicies/twitter-law-enforcement-support.

Viber

BASIC INFORMATION[54]

Viber is an application that allows for the exchange of messages and calls, both audio and video. The company, founded in Israel, was acquired by Japan's Rakuten in 2014.

Since 2017, its corporate name is Rakuten Viber. Viber can be used on Android, iOS, Windows desktop, Mac and Linux.

Registration requires a valid phone number, which will be verified via SMS or phone call with an activation code. Phone numbers can be changed at a later moment. When Viber is set up on a phone, the Viber account can be connected to other social network accounts, in particular, Facebook, Twitter or VK.

CONTACT INFORMATION

Viber Media
S.àr.l. 2, rue des Fossé, L- 1536 Luxembourg
Grand Duchy of Luxembourg

Viber Support page: https://help.viber.com/en/contact
(Select 'Inquiry category': Call History (CDR) Request)

LAW ENFORCEMENT INFORMATION

Public guidelines for law enforcement requests are not available.

[54] Excerpt cited from the SIRIUS Europol Platform for Experts

VK

BASIC INFORMATION[55]

VK (short for its original name VKontakte or ВКонтакте, meaning InContact) is an online social media and messaging service headquartered in Saint Petersburg, Russian Federation. It is available in several languages, but it is particularly popular in Russia, where it ranks as second most popular website, as of January 2019[56]. Counting almost 100 million monthly active users[57], the platform's main features are similar to other social media platforms, including private messaging, connecting with friends and posting text, pictures, documents and links.

CONTACT INFORMATION

LLC "V Kontakte", prem. 1-N, bld. 12-14, Lit. A, Khersonskaya st., St. Petersburg, Russia, 191024.

LAW ENFORCEMENT INFORMATION

Russian national legislation[58] does not allow the disclosure of data held by private companies based in the country directly to foreign authorities. This also applies to emergency circumstances.

Encryption of services: Under Russian national legislation, OSPs are obliged to provide the state security agency with decryption information for electronic messages[59].

Here you can find more information in English.

WeChat

BASIC INFORMATION[60]

WeChat is a Chinese multi-purpose messaging, social media and mobile payment app developed by Tencent. First released in 2011, it became the world's largest standalone mobile app in 2018, with over 1 billion monthly active users. WeChat has been described as China's "app for everything" and a "super app" because of its wide range of functions. WeChat provides text messaging, hold-to-talk voice messaging, broadcast (one-to-many) messaging, video conferencing, video games, sharing of photographs and videos and location sharing[61].

[55] Excerpt cited from the SIRIUS Europol Platform for Experts

[56] Russia beyond, February 2019, Facebook and Google's Russian rivals: Why are they winning?, accessible at https://www.rbth.com/science-and-tech/329970 – [accessed 02.06.2021]

[57] VK.com, accessible at https://vk.com/about [accessed on 02.06.2021]

[58] Constitution of the Russian Federation, Federal Law of 27.07.2006 № 152-ФЗ, Directive of the President of the Russian Federation of 22.03.2008№144-pnandFederal Law of 12.08.1995 г. № 144-ФЗ as amended on 06.07.2016, accessible at https://pd.rkn.gov.ru/authority/p146/p164/

[59] The Moscow Times, October 2016, Russia Begins Search for Decryption of Online Messengers, accessible at https://www.themoscowtimes.com/2016/10/04/russia-begins-search-for-decryption-of-online- messengers-55585 [accessed 07.06.2021]

[60] Excerpt cited from the SIRIUS Europol Platform for Experts

[61] Technisia.com – Messaging apps should reveal monthly active users, accessible at – https://www.techinasia.com/messaging-apps-should-reveal-monthly-active-users [accessed on 09.06.2021]

User activity on WeChat is analyzed, tracked and shared with Chinese authorities upon request as part of the mass surveillance network in China. WeChat censors politically sensitive topics in China. Data transmitted by accounts registered outside China is monitored, analyzed and used to build up censorship algorithms in China[62].

CONTACT INFORMATION

Ms. Elizabeth Byun
Head of Legal and Compliance
Level 29, Three Pacific Place, No.1 Queen's Road East,
Wanchai, Hong Kong
policy@wechat.com

LAW ENFORCEMENT INFORMATION

LAW ENFORCEMENT DATA REQUEST GUIDELINES are available here:
https://www.wechat.com/en/law_enforcement_data_request.html

A Legal_Process_Request&Preservation_Request_Formas well as an Emergency_Disclosure_Request_Form are also available and shall be addressed to: lawenforcement@wechat.com

WhatsApp[63]

BASIC INFORMATION

WhatsApp is the most used freeware, cross-platform, end-to-end encrypted instant messaging application in the world. WhatsApp is available for Android, iPhone, Windows Phone, Blackberry, Nokia, Mac and Windows PC. Its main functionalities include online messaging/chat between two or more users (group chat), free internet phone calls, video calls, multimedia sharing (image, video, audio, documents) and locations.

CONTACT INFORMATION

Different legal entities are considered to be data controllers for different countries/regions:
For residents in the European Economic Area:
WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour Dublin 2, Ireland

For rest of the world residents:
WhatsApp Inc., Law Enforcement Response Team 1601 Willow Road, Menlo Park, California 94025, United States of America

Law Enforcement Online Request System:
https://www.whatsapp.com/records/login

E-mail address for general inquiries from law enforcement:
records@records.whatsapp.com

[62] ˙Fastcompany.com – How Social Cash Made WeChat The App For Everything, accessible at https://web.archive.org/web/20170103135948/https://www.fastcompany.com/3065255/china-wechat-tencent-red-envelopes-and-social-money [accessed on 09.06.2021]

[63] Excerpt cited from the SIRIUS Europol Platform for Experts

LAW ENFORCEMENT INFORMATION

WhatsApp Inc. is part of the Facebook Inc. company. However, WhatsApp and Facebook legal and law enforcement response teams are not the same.

Requests for data preservation and disclosure regarding WhatsApp users should not be addressed to Facebook Inc. WhatsApp uses a customized version of the open standard Extensible Messaging and Presence Protocol (XMPP).

WhatsApp guideline for law enforcement is available at: https://faq.whatsapp.com/en/android/26000050/?category=5245250

WICKR[64]

BASIC INFORMATION

Wickr is an American software company based in New York City. The company is best known for its instant messenger application of the same name.

Wickr has developed several secure messaging apps based on different customer needs: Wickr Me, Wickr Pro, Wickr RAM, and Wickr Enterprise. The Wickr instant messaging apps allow users to exchange end-to-end encrypted and content-expiring messages, including photos, videos, and file attachments. The software is available for the iOS, Android, Mac, Windows, and Linux operating systems.

CONTACT INFORMATION

For business inquiries, contact:
Wickr, Inc.
254 W 31st St, New York, NY 10001, USA
(415) 286-9476

LAW ENFORCEMENT INFORMATION

Legal process guidelines are available here.

Law enforcement officers can submit an emergency disclosure request via email: legal@wickr.com.

[64] Google Play – Wickr Me – Private Messenger, accessible at https://play.google.com/store/apps/details?id=com.mywickr.wickr2 [accessed on 04.06.2021]

Youtube

BASIC INFORMATION

YouTube is an online video sharing and social media platform owned by Google. Over the years, YouTube has expanded beyond the website into mobile apps, network television, and to permitting other services like Discord and Nintendo to access YouTube. The range of videos on YouTube is seemingly infinite.

Please also refer to the privacy policy and the terms of service.

More information on how Google handles government requests for user information can be found here. Contact Information and Law Enforcement Information See Google.

Zalo[65]

BASIC INFORMATION

Launched in 2012, Zalo is Vietnam's premier chatting platform, with more than 100 million users worldwide. Daily, people send about 900 million messages, make 50 million minutes of calls, and deliver 45 million pictures through the app. Zalo Pay feature was introduced in 2017.

It is an app that incorporates many functions and features, from social networking and e-commerce, to goods delivery, and financial services.

CONTACT INFORMATION

ZALO
322B Ly Thuong Kiet, P14, Q10, Ho Chi Minh City
Vietnam

LAW ENFORCEMENT INFORMATION

Zalo state that they do not share any data with third parties.
Please find here the policy.

[65] Quoracreative.com, updated on December 2019 – How is Zalo challenging Facebook Messenger, WhatsApp, and Viber in Southeast Asia, accessible at https://quoracreative.com/article/zalo-app [accessed on 04.06.2021]

Annex II: Recommendations for handling seized mobile communication devices

Background

Annex 2 accompanying the joint Europol-Frontex intelligence notification on Digitalisation of migrant smuggling includes a list of practical guidelines for handling seized mobile communication devices, as provided by specialists from Europol's European Cybercrime Centre and experts within the European Migrant Smuggling Centre, complemented by recommendations available in open sources.[66]

Checklist for facilitating forensic extraction of mobile communication devices

The following information serves as guidance when a mobile device is seized for forensic examination / data extraction:

- The device should be left in the state it was identified, whether the device has been found switched on or off. Unnecessary handling should be avoided. Any actions taken should be fully documented.
- The device should, ideally, be stored in a Faraday bag, to prevent it from connecting to any networks (cellular or Wi-Fi).
- If turned on, arrangements should be made for it to be set into flight mode to prevent the alteration of data and/or remote access/wiping. Provisions should be made to keep the device charged, e.g. by using a power bank or keeping the device plugged into the mains. In the eventuality that it is not possible to enable the flight mode on the device, then this should be connected to a power bank and everything (including charging cable) should be placed inside a Faraday bag, adequately closed. The advice of a forensic practitioner should then be sought.

[66] Scientific Working Group on Digital Evidence's (SWGDE), 2013, Best Practices for Mobile Phone Forensics, accessible at https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Best-Practices-for-Mobile-Phone-Forensics-020113.pdf ;
Infosec Institute, 2019, The mobile forensics process: steps and types, accessible at https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/;
Forensics Colleges, 2021, Mobile forensics: How digital forensics experts extract data from phones, accessible at https://www.forensicscolleges.com/blog/guide-to-mobile-forensics;
International Journal of Computer Science and Security (IJCSS), Volume (13): Issue (5) : 2019, Smartphone Forensic Challenges, accessed at https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume13/Issue5/IJCSS-1501.pdf. All open sources have been accessed on 09.06.2021

- In case the device is turned off, it should not be opened in search for the IMEI. This parameter will be identified during the forensic examination/extraction. A note should be made of the make and model (if visible).
- Ideally the charger and associated cable (s), memory cards, loose SIMs should be seized along with the phone.
- A chain of custody or evidential continuity should be in place, from the moment the item is seized. The seizure report with the holder's personal details, including the place and time of seizure, should be attached to the device.
- To facilitate a successful forensic extraction the following data should be retrieved whenever possible, either by addressing this matter to the user or by way of special tactics:
  - Device password or pin code;
  - Security pattern;
  - SIM card PIN.

FRONTEX

EUROPOL

Frontex – European Border and Coast Guard Agency
Plac Europejski 6, 00-844 Warsaw, Poland
T +48 22 205 95 00
F +48 22 205 95 01
frontex@frontex.europa.eu
www.frontex.europa.eu

Europol, Operations Directorate
P.O. Box 908 50
2509 LW The Hague
The Netherlands
T:+31 70 302 5000
https://www.europol.europa.eu

Ref. No.:
Frontex – European Border and Coast Guard Agency

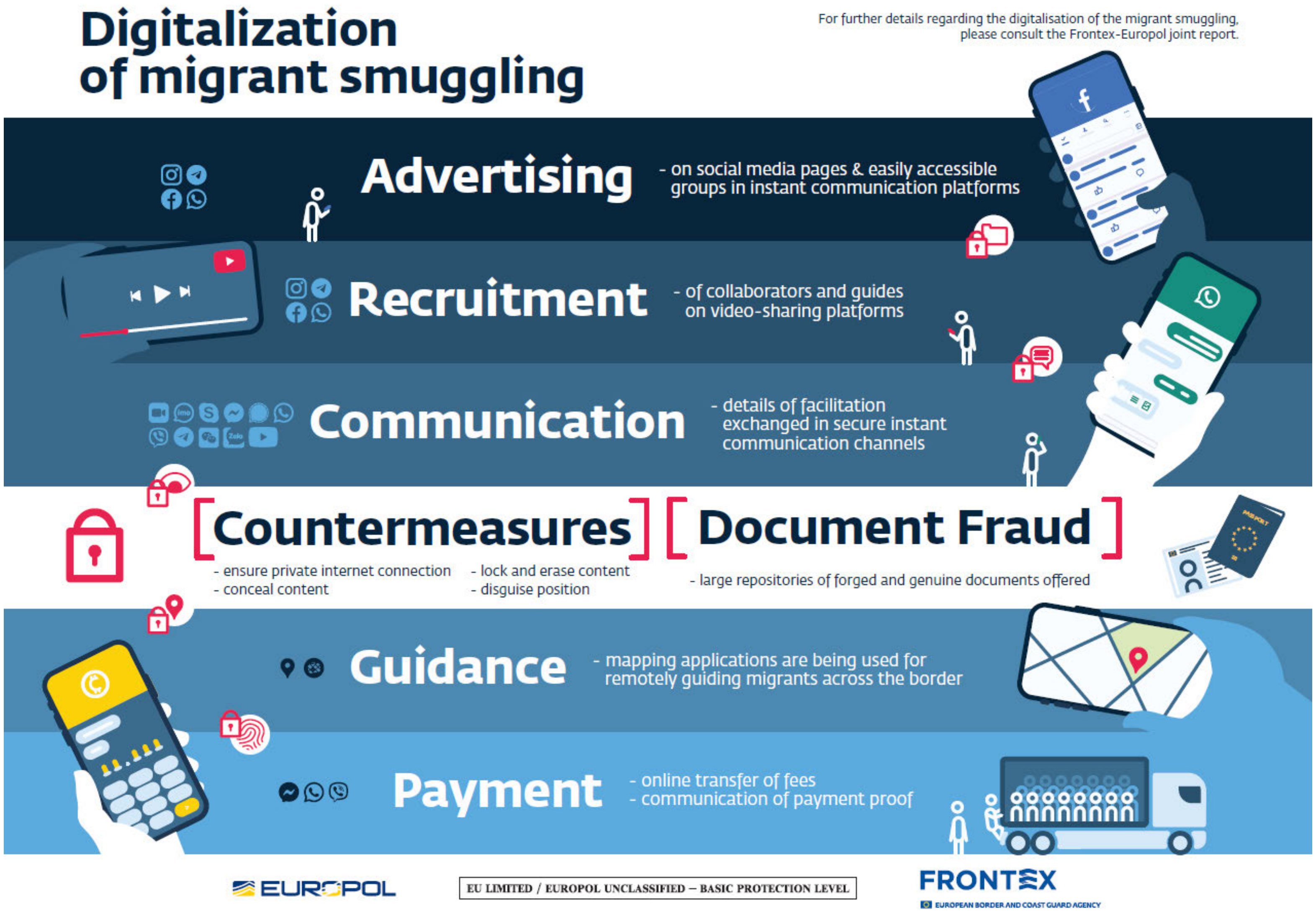
The Hague, July 2021
Ref. No.: IN 2021-223

Book:
TT
ISBN
doi:

PDF:
TT
ISBN
doi:

FPI: 21.5049

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL



Digitalization of migrant smuggling

For further details regarding the digitalisation of the migrant smuggling, please consult the Frontex-Europol joint report.

Advertising

- on social media pages & easily accessible groups in instant communication platforms

Recruitment

- of collaborators and guides on video-sharing platforms

Communication

- details of facilitation exchanged in secure instant communication channels

[Countermeasures]

- ensure private internet connection
- conceal content
- lock and erase content
- disguise position

[Document Fraud]

- large repositories of forged and genuine documents offered

Guidance

- mapping applications are being used for remotely guiding migrants across the border

Payment

- online transfer of fees
- communication of payment proof

EUROPOL

EU LIMITED / EUROPOL UNCLASSIFIED – BASIC PROTECTION LEVEL

FRONTEX

EUROPEAN BORDER AND COAST GUARD AGENCY