Cybercrime@EAP III

Public/Private Cooperation under the Partnership for Good Governance with Eastern Partnership countries

2016/DGI/JP/3608
30 August 2017

Study on Strategy of Cooperation with Multinational Service Providers

Prepared by Council of Europe experts
under the Cybercrime@EAP III Project

www.coe.int/cybercrime

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Email cybercrime@coe.int

Disclaimer
This review has been prepared by independent Council of Europe experts Albena Spasova and Nigel Jones with the support of the Cybercrime Programme Office of the Council of Europe.
This document has been produced as part of a project co-funded by the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party.

Contents

1 Introduction

Cooperation between criminal justice authorities and private sector entities, including in particular service providers, is essential to protect society against crime. Such cooperation concerns primarily access by police and prosecution services to data held by service providers for criminal justice purposes, but also the sharing of information and experience, as well as training. As the Eastern Partnership region becomes increasingly integrated into the global economy and with increasing number of people from these countries with daily access to cyberspace, the law enforcement often faces the fact that the multinational service providers (Amazon, Apple, Facebook, Google, Microsoft, PayPal and similar) are in possession of information that can be used as evidence in cases of cybercrime drives the demand for more effective access to potential evidence in the cloud. The increasing use of multinational platforms poses new challenges in front of law enforcement authorities when conducting investigations. These challenges are related to the level of knowledge on how these platforms function and also what data they store about their users and procedures applied for sharing such data.

Effectiveness of access to such information is largely dependent on the success of direct cooperation of the law enforcement with such companies, as there are more opportunities to get access to potential evidence through voluntary cooperation mechanisms rather than reverting to more time-consuming process of mutual legal assistance. However, we should keep in mind that direct cooperation is entirely based on the voluntary participation of the service provider and not all data could be obtained following this direct cooperation mechanism. Direct cooperation should be envisioned as an exception rather than a rule from the law enforcement standpoint.

At the same time, voluntary nature of direct cooperation with foreign/multinational companies is a difficult concept to grasp for law enforcement agencies of the Eastern Partnership who are used to unhindered application of powers to compel Internet service providers into cooperation. Effective communication with the globally present and economically powerful companies with entirely different business models and modes of operation requires different thinking and skills on the part of the law enforcement officers, as the recourse to national methods of coercion through criminal procedure or general police powers may not be applicable or is not feasible in terms of the need for expedited access to such data. The lack of knowledge is particularly acute in terms of understanding the logic of such cooperation from the industry perspective and knowing realistic expectations from the business sector as it comes to the readiness to cooperate with the law enforcement overseas. For the success of such cooperation, we need to aim for the maturity of relationships between the multinational companies and law enforcement and achieving this maturity is not limited only to the process of sending requests for information and receiving feedback. The maturity of these relationships is a multi-layered process which starts with better understanding of each other's needs and operational rules and goes through information sharing and training for improving knowledge.

Cooperation between industry giants and governments is challenging and we are witnessing that sometimes the lack of such cooperation can go too far. Recent example include tension between FBI in the USA and Apple for disclosing encrypted data[1] and an example from

[1] Explanation about the recent argument between the FBI and Apple was addressed in a letter release on the company's website addressing all Apple customers on February 16, 2016. In the letter there is Apples stand point about the need for encryption, details about the San Bernardino Case which created the conflicting positions between FBI and Apple and why there is threat to data security and about the dangerous precedent. Letter could be found on this link. https://www.apple.com/customer-letter/

Germany how law makers could fine up to 50 million euros[2] for Silicon Valley companies that do not limit the circulation of hate speech.

The above examples are provided to show the complexity of relationships between multinational companies and government authorities worldwide, and to emphasise once again on the importance of developing a mature cooperation model among law enforcement authorities and multinational service providers with the purpose to increase the level of access to electronic evidence in a timely manner. This is important, because in the global economy market we witness that most of the crime is committed with the use of technology and this requires cross-border exchange of information for successful investigations and prosecutions.

2 Purpose of the study

Carried out under the Cybercrime@EAP III project aimed at improving public/private cooperation on cybercrime and electronic evidence in the Eastern Partnership region, the report offers insight into opportunities for effective cooperation between the law enforcement of the EAP and the multinational service providers.

The overall purpose of this report is to evaluate the current direct cooperation mechanisms between law enforcement authorities in EAP region and multinational service providers with the aim to provide solutions on how to strengthen direct cooperation and increase the number of responses to requests. At this stage, some law enforcement agencies experience difficulties to receive information in criminal cases from multinational service providers when using the direct communication channels, which prevents them to solve a criminal case in a timely manner. This study will attempt to analyse the existing methods for cross-border cooperation among law enforcement and multinational service providers, identify bottlenecks and propose solutions for timely exchange of information and protection of individuals' privacy.

The report does not seek to repeat other reports and intends to complement them. Documents such as the following may be useful to be read in conjunction with this report:

- *The Final report of the T-CY Cloud Evidence Group "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY";*[3]
- *T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention).*[4]

3 Background

Criminal investigations require access to evidence in many forms, including witness testimony, physical objects, documents and in recent years - electronic evidence. There is often an assumption that this is a new requirement, yet, in many countries it has been a

[2] "The German parliament has voted in favour of a law that includes the provision to levy fines of up to €50 million (£44m) from popular companies such as Facebook and YouTube if they fail to remove hateful posts in a timely manner. The law, which is due to come into effect in October, affects sites with more than 2 million users nationally. It requires internet giants to find and delete posts containing "evidently unlawful" abusive material within 24 hours to avoid being hit with a penalty. It also mandates companies delete hateful material that isn't unlawful within seven days. " More information can be found in this article: http://www.telegraph.co.uk/technology/2017/06/30/germany-fine-facebook-youtube-50m-fail-delete-hate-speech/,

[3] https://rm.coe.int/16806a495e

[4] https://rm.coe.int/16806a495e

constant for more than two decades. At national level, the challenges of dealing with electronic evidence have been met through cooperation between criminal justice system players and the holders of such evidence - primarily service providers who hold information about their customers, often needed by law enforcement. In some countries, this has led to legislation that governs access to such data.

The concept of international investigations and cross-border requests for data has not yet seen rules developed to allow for rapid and lawful access to data. Until recently, most MSP's held their data in the US, except for non-US data, which is often held in Ireland. Nowadays, data storage may be cross- or multi-jurisdictional, with the advent of cloud services and storage. This leads to a situation where it may be possible that the MSP may not know exactly where data is held on a daily basis. Reliance on cooperation from MSP's who receive and adjudicate whether they will release requested data brings new challenges. Although this report is primarily aimed at the countries of the Eastern Partnership and their experience, there is limited data available for that particular region and the wider picture is equally important.

This report examines the issue from the perspective of both data holders and data requestor and provides conclusions and concrete recommendations to improve the current situation. Cross-border cooperation in criminal cases among non US law enforcement authorities and multinational service providers based in the US needs to be improved, because very often legitimate law enforcement authorities cannot access digital evidence hold by a foreign service provider. This lack of access to electronic evidence hampers criminal investigations and leads to increasing criminal behaviour which is unpunished. On the other hand, multinational service providers are encountering restrictions for sharing personal data and are unable to provide support to law enforcement to access the necessary electronic evidence. We should also consider the access to digital evidence in a timely manner by law enforcement because the traditional methods for exchanging cross-border evidence in criminal cases is time-consuming and cumbersome, and does not allow law enforcement to have access to the digital evidence in due time.

Currently information from one country is shared with another country in the following manner:

- **Mutual Legal Assistance Treaties:** this official method for exchanging information is based on legal treaties signed by the two countries and uses the diplomatic channels for exchanging information. In this report we will not analyse the MLAT process, but rather focus on the difficulties which lead in delays for obtaining the necessary data requested. These delays are the result of few circumstances:
    - Increasing number of data requests sent to the U.S. Department of Justice (most of the multinational service providers are based in the US and thus sharing of information is performed through the diplomatic channels of the Department of Justice)
    - Manual process for handling cross-border cooperation which slows down the information sharing

- **Direct cooperation** between law enforcement authorities and multinational service providers:
    - This is voluntary mechanism for sharing information and usually multinational service providers will share only information for serious crimes and for criminal behaviour which poses some imminent threat.
    - Restrictions for US based multinational service providers to share information with non US law enforcement. This restriction is based on a law from 1986 called Electronic Communication Privacy Act. When this law was created the

technological world was very different and there were no global technology giants like Google, Facebook, AirBNB and others providing variety of services to citizens outside the United States. This restriction is a result of a so called "blocking" procedure which does not allow US service providers to share content with law enforcement agencies outside the Unites States. Such blocking procedures also exist in other territories which makes it difficult to share cross-border information in criminal case. These restrictions differentiate emergency cases as an exception from this prohibition.

- **Information obtained from open source:** very often law enforcement rely on open source intelligence techniques for obtaining information in a criminal case. Such methods allow law enforcement to obtain better search results when using a search engine, use alternative search engines, search within social networks, search online maps, people search engines, online communities, documents, photographs, videos, IP addresses and domains, government records, radio frequency monitoring, APIs and software applications. This is a reliable method for obtaining information online, but information obtained could not be used as evidence in Court.

- **Privacy of individuals**: this is another aspect which is critical in cross-border cooperation. Very often multinational service providers will not comply with a request for direct data exchange if they have suspicious about the fact that privacy might be jeopardized and human rights violated. This said here means to emphasize on the fact that countries need to revisit their legislation in the area of privacy, due process and human rights protection. This is largely relevant for countries with poor human rights record.

4 How multinational service providers operate

The era of Google, Facebook, Amazon, Netflix, Uber is upon us. It is also the era of big data or everything data. In this landscape, law enforcement authorities, in order to be successful in obtaining data from the multinational providers, need to think and operate differently. In criminal cases, one-way communication is not an applicable formula and law enforcement need to learn that communication for resolving a criminal case online is a two-way street. In this regard, when law enforcement request information about a criminal case directly from a multinational service provider, they should also provide sufficient background information about the criminal case they are requesting information for. In addition to this, they need to have a good understanding about the platform from where they request information functions.

We live in an era where the market leaders are those companies which make the gathering and analysis of customers' data a priority. This is to say that guarding this data and customer interest is key priority for market leaders. Thus, investment in capabilities in dealing with law enforcement requests is not a priority for all MSPs and we witness different levels of commitment. The majority of companies' budgets are oriented for innovation and transformation of market and very little is left for law enforcement cooperation. There is a clear need on behalf of some providers to raise the level of commitment, to create or strengthen companies' capabilities when dealing with law enforcement requests. Understanding how law enforcement works and why data is important for them would better decision-making in this context. This could be achieved if a dialogue is initiated and communication between law enforcement and MSPs is sustainable.

4.1 How these entities are incorporated

Most of the multinational service providers are based in the United States but provide services for individual customers worldwide.

Some multinational service providers like Microsoft[5] have national offices in almost every country from the EAP region. It should be noted that those offices are representing only the business units for Microsoft and could be contacted in relation to services and products offered by the company on the national market. If they do not have an establishment in a particular country, the nearest regional office could be contacted. These national divisions are usually not entitled to deal with law enforcement requests and are not a communication channel for law enforcement to deliver the request for information to the headquarters or the regional European office entitled to deal with law enforcement requests. Companies like Google for example do not have establishments on the national markets and operate through their regional offices.[6] Usually the European headquarters entitled to deal with law enforcement requests are based in London, Dublin, Luxembourg or other European cities.

Instead, multinational service providers are encouraging law enforcement to contact them using MSPs' online platforms. This process helps them address presumably lawful requests for data and also avoids further delays. However, very often law enforcement using online platforms do not receive responses or any feedback why their request is not responded to. This leads to unsolved criminal cases and justice is not served, witnesses to the crime become unavailable or the data available is destroyed. To address this, law enforcement need to receive some feedback when they use the online platforms for requesting information since this seems to be the only available channel of communication with multinational service providers since they do not have office opened in the respective EAP countries. All requests should be in English language and with the necessary credentials as required by the particular multinational service provider. When a request is received through the online channel, it is reviewed by an employee who considers if the request is legitimate or not. Usually the team responsible for law enforcement requests are divided not by countries but by regions; thus it is very difficult for them to understand the particularities of every jurisdiction from where they receive information. Usually, if a request is denied, no feedback is sent to the law enforcement officer whose request was denied.

The major lesson to be learnt by law enforcement and multinational service providers is that keeping online platforms safe is a joint responsibility of law enforcement, businesses and users. The old model and perception that law enforcement are solely having the responsibility to fight crime and industry's responsibility is to only to provide services needs to change. There is a need to jointly identify activities and partnerships in order to limit the illegal activities on the internet platforms and the illegal use of digital channels for distribution of illegal content or communication of illegal activities. This could be achieved only with joint sustainable efforts focusing on developing a mature cooperation model. However we are still witnessing multinational companies with limited interest in cooperation with law enforcement and also in developing capabilities to cooperate with law enforcement.

All analysis until now is focusing on the rules which multinational providers are applying when it comes to cooperation with US or international law enforcement authorities. It is of equal importance to also look into law enforcement capabilities for direct cooperation as well. Thus further in this report we will focus on MSPs concerns and needs as well.

[5] In the following link you could find information about Microsoft European offices: https://www.microsoft.com/worldwide/region.aspx?region=Europe

[6] In this link you could find information about the European offices for Google: https://www.google.com/intl/en/about/locations/?region=europe

For example, where there is a terrorism case where fast reaction is needed and a service provider identifies information on their platforms which they need to communicate to law enforcement in EAP countries, it is very difficult to identify a point of contact to which information should be communicated. Thus, it is equally important to determine a land line and address to be used by service providers in emergency cases for contacts with law enforcement. It is also important to emphasize on the language skills for the law enforcement officers in charge of the POC, since MSPs preference would be communication in English language.

4.2 How companies process data

It is also important to have a better understanding how these businesses operate. The market leading companies are basing their business model on data. It is their competitive advantage in comparison with other traditional business models. Customer data and data provided by customers helps them in making the right business decisions and provide services and products which customers want. Thus, it is of crucial importance for them to protect data. On the other hand on these platforms there is data publicly available which could be accessed by law enforcement and help them in the investigation.

For example: If you conduct investigation on eBay, the following tips are for law enforcement agencies to assist in your investigation:

- Search for active listings using search string or specific item number: Lets you search by nearest zip code using search options on left hand column.
- Search by seller ID for all active/completed sales, dating back 30 days: Generally provides you with the seller's state of residence.
- Feedback Profile reflects comments made by other users regarding prior transactions.
- Create your own Favorite Searches
- eBay listings remain visible on the site for about 90 days after closing, and are searchable by specific item number.

Example of Facebook searches: there are lots of tips how to identify necessary information by applying search tips. This search option is called Facebook Graph. It is a search engine which Is integrated within Facebook social graphs.[7] Whining a social graph individuals and their behaviour acts are looked at as nodes and could be correlated. At Facebook it is easy since we as individuals could be linked to other individuals or interest groups or behaviours based on data which we provide.

For example we could apply graph search:

- If we are searching for a particular ad;
- Pictures of friends before a certain period;
- Single man/women in a geographic area;
- Restaurants my friends like.

This search method is often used by marketers to identify their targets. Law enforcement could potentially use this method for obtaining additional information, but information acquired in this manner does not represent digital evidence.

That's why law enforcement should not solely rely only on data received by service providers but should use open source intelligence techniques to obtain the necessary data for their

[7] More information about what is a social graph and how could be used can be found on this link: http://whatis.techtarget.com/definition/social-graph

investigation. This could be achieved only when there is a basic understanding how the different platforms work.

To better understand the digital landscape, we need to understand the development of the digital channels, the functioning of the powerful distributers to content and social networks and the development of advanced computing and cloud services. Since this landscape is very volatile it might be difficult for law enforcement to keep up with this pace of change.

It is useful to remind the reader of the types of data that are referred to in this report.

4.3 Treatment of different categories of data

While the Cybercrime Convention does not define electronic evidence, it nevertheless differentiates between 'subscriber information', 'traffic data' and 'content data', which are most often used types of such evidence. These types of computer data are subject to different procedural powers and corresponding conditions and safeguards. For example, access to subscriber information, as well as traffic data, has less negative impact of person's private life and fundamental rights and freedoms, so conditions to allow it can be lower than with regard to the content data, which should enjoy highest legal protection.

Subscriber information is defined in Article 18(3) of the Convention, as:

> *any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
> *a) the type of communication service used, the technical provisions taken thereto and the period of service;*
> *b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
> *c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

The notion of "traffic data" is used in the Convention, but also in EU Directive on privacy and electronic communications[8] and many national sources of law. It should be noted that definitions in these sources differ and that they are differently applied in different areas of law. According to Article 1(d) of the Convention, **traffic data** means:

> *any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*.

Such data is in possession of service providers, which are defined in Article 1(c) of the Convention as:

> *i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and*
> *ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.*

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

The notion of **content data** is relevant since it is subject to Convention's most intrusive procedural power – interception of content data, defined in Article 21. While the term 'content data' is not defined in the Convention itself, according to Explanatory report it refers to "content of the communication" or "information being conveyed by the communication (other than traffic data)".[9]

Most jurisdictions have legislation in place that allows for lawful access to data, including data held by national service providers. This is usually by way of a judicial production order issued by a judge or magistrate, on request from a prosecutor or law enforcement official, conducting a criminal investigation. Some countries allow for emergency situations where data may be obtained in expectation of and a requirement to obtain a retrospective production order.

The issue of obtaining data from service providers has become contentious and as a result the Cybercrime Convention Committee T-CY has issued a guidance note on Production Orders for Subscriber Information.[10]

It is not the purpose of this report to simply reproduce the content of the guidance note or the Final report of the T-CY Cloud Evidence Group into criminal justice access to electronic evidence in the cloud, and the recommendations for consideration by the T-CY that was an influence in the issuance of the guidance note.[11] It is recommended that readers of this report consider the contents of the above documents, in conjunction with this document to gain a full picture. This report is examining the practical issues pertaining to cooperation with Multinational Service Providers (MSP's) only.

When dealing with MSP's, it should be remembered that they have their own policies and practices in dealing with requests for **subscriber information** from law enforcement and these are dealt with, elsewhere in this report. Most, if not all MSP's have legal departments that check any incoming requests. Amongst other things, they check the legislation in the requesting country, to ensure that the request would be lawful in that country. If there is a requirement at the domestic level in the requesting country for the issue of a production order for obtaining the requested data at the domestic level, the MSP will expect that there is a domestic order in place for the data that is being requested from them. In other words, there is no point in submitting a request for data from an MSP, if the relevant provisions in domestic legislation have not been fulfilled.

It is also important to consider that most of the basic subscriber information is provided by the individual signing up for the service and is not always accurate. MSP usually disclose in direct cooperation only this category of data. For the other types of data described below law enforcement is required to follow the international legal procedures based on mutual legal assistance. It is also important to note that MSPs will respond to direct requests providing basic subscriber information usually if the described case for which law enforcement is requesting information has an element of urgency or threat. This should not be confused with the special procedures which MSPs developed for dealing with emergency requests. This relates to usual direct requests for data.

As regards **traffic data** will usually be disclosed by a MSP only on the basis of MLA process and not as a result of direct cooperation. This is due to the fact that in practice, taking into account the voluntary nature of disclosure through direct cooperation channels, these channels are deemed fit for the exchange of information that needs to be accessed

[9] Explanatory report, para 209.

[10] https://rm.coe.int/16806a495e

[11] https://rm.coe.int/16806a495e

expeditiously (i.e. subscriber information). Therefore, law enforcement should be aware of the fact that there is a slim possibility of getting access to traffic data through direct cooperation mechanisms, and thus have to be prepared to launch a mutual legal assistance request.

Similarly, **content data** will usually be disclosed by a MSP only on the bases of MLA process and not as a result of direct cooperation.

It is important to mention that all three categories of data could be obtained from the MSPs following the international legal standards for cooperation (primarily mutual legal assistance). However this process is not very efficient and usually time consuming and law enforcement are relying more and more on the direct cooperation model. However it should be considered that the direct cooperation is entirely based on the free will and capability of the service provider to provide the data. Thus it is not encouraged to solely use this method for obtaining information for the case. The purpose of this report is to describe the needs and concerns by both parties and seek solutions for improving the level of cooperation overall and in particular, direct cooperation.

5 Concerns related to cooperation

As demonstrated in the previous section of the study, the existing procedures for international cooperation in criminal matters may not be the best options to obtain access to data held by multinational service providers. Direct cooperation channels thus become more important; however, as these are based on free will of the companies, having a look at the concerns that may affect such cooperation could be useful.

5.1 Multinational Service Providers Concerns

Dealing with law enforcement is challenging for the global companies for several reasons and their concerns fall broadly into the following categories:

- Low level of understanding about the business model by law enforcement. Multinational service providers provide variety of services and very often law enforcement are not familiar with them and how data in respect of these services may or may not be available. The lack of knowledge about a platform might have direct implications for a successful investigation. From multinational service provider point of view, better understanding about the services offered and mechanisms of data gathering process will help law enforcement in drafting better requests

- Maturity of the cooperation model between service providers and law enforcement has direct implications on the quality of the requests. It is advised for law enforcement to seek direct contact with service providers and build trusted relationships. This will increase their knowledge about the platform and as well will help them draft better data requests.

- Protection of human rights and abuse of power – if a request comes from a country with a poor human rights record, a request for data might be subject to a higher scrutiny. This might not be publicly announced in the multinational service providers' policies, but is usually a consideration to take into account. In such situations it will be advisable to use the MLATs for requesting information.

- Multinational service providers have different level of commitment when dealing with law enforcement requests. Some providers do not have this infused in their management and thus have not build capabilities to deal with law enforcement request directly.

- Bad quality of requests: the reasons for a data request refusal could vary but the most often one is incomplete requests. To avoid this it is advisable for law enforcement to undergo training how to build a data request with multinational providers.

5.2 Law Enforcement Concerns

Dealing with MSP's is challenging for law enforcement for several reasons and their concerns fall broadly into the following categories:

- Varying policies of MSP's in dealing with requests and, as a consequence, different response levels to different countries from different MSP's. For example, the response rate to the Netherlands is over 80% from Google and Microsoft, whereas Yahoo does not respond at all to requests from the Netherlands.

- The uncertainty of whether any response will be received from some MSP's. It has been described by some as a "lucky dip" in that a request is submitted and relies entirely on the decision of a private sector organisation as to whether data will be released.

- Many MSP's provide no response at all to some countries, leading them to the view that MSP's are making decisions based on their view of a country rather than a legal basis.

- No feedback is provided by MSP's as to the reason for refusal. In some instances, it may be administrative rather than substantive and capable of being rectified.

- One major concern to law enforcement is the disclosure policies of the MSP's. Examples were given in the recent COE "training programme on International Cooperation, including multinational ISP's, for the Eastern partnership region", where countries made direct request to MSP's when confronted with the potential that the individual personal information, including name, rank, position, email address and phone number, may be released to terrorist suspects as a result of the disclosure policy. They were not able to receive any assurance from the MSP's that their personal data was secure. This is an issue that cannot be solved with this report, other than being raised in the conclusions and recommendations.

- While the issue of lawful access to data held by MSP's in largely confined to those based in the USA, the issue of data exchange with service providers in other countries is often mentioned by law enforcement.

5.3 Current attempts to solve these concerns

The **Council of Europe**, through the work if its Cloud Evidence Group (CEG), already referenced above, has sought to bring some clarity to the challenges of recognising and

collecting evidence in the cloud that is often located outside the jurisdiction where lawful access to data has been granted. The final report of the CEG sets out some recommendations, including one for the COE to develop a Guidance note on the issue of production orders. This guidance note has been issued in June 2017[12] and is covered and referenced elsewhere in this report.

The Cloud Evidence Group in 2016 submitted the following recommendations to the Cybercrime Convention Committee (T-CY), which were adopted by the Committee in its 16th Plenary:

1. To invite Parties and Observer States to ensure follow up to the T-CY Recommendations on MLA adopted in December 2014 and falling primarily under the responsibility of domestic authorities, that is, Recommendations 1 to 15; the T-CY to assess progress made, and capacity building programmes, if necessary, to support implementation.

2. To consider the draft Guidance Note on Production Orders for Subscriber Information as appended to this report in view of adoption and in view of offering guidance to Parties in the implementation of Article 18.

3. To invite Parties and Observer States to review domestic procedures for access to subscriber information and thus to ensure full implementation of Article 18 Budapest Convention.

4. To take practical measures – pending longer-term solutions – to facilitate more coherent cooperation between service providers and criminal justice authorities, in particular with respect to the disclosure of subscriber information upon a lawful request in a specific criminal investigation but also with respect to emergency situations.

5. To consider the preparation of a draft Protocol to the Budapest Convention with the following elements:

- Provisions for more effective mutual legal assistance
  - a simplified regime for mutual legal assistance requests for subscriber information;
  - international production orders;
  - direct cooperation between judicial authorities in mutual legal assistance requests;
  - joint investigations and joint investigation teams;
  - requests in English language;
  - audio/video hearing of witnesses, victims and experts;
  - emergency MLA procedures.
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.
- Clearer framework and stronger safeguards for existing practices of transborder access to data.
- Safeguards, including data protection requirements.

During the 17th Plenary of the T-CY in June 2017, the Committee adopted the Terms of Reference for the preparation of a draft Second Additional Protocol to the Budapest Convention on Cybercrime, and tasked Cloud Evidence Group to work in this direction.

[12] http://rm.coe.int/doc/09000016806f943e

Also worthy of note is that on 8 June, the **European Commission** presented to EU Justice Ministers a set of practical and legislative options[13] to improve cross-border access to e-evidence.

Among the problems of lawfully accessing data in other jurisdictions are:

- In cross-border cases, law enforcement and judicial authorities tend to cooperate using mutual legal assistance procedures or the European Investigation Order. However, these traditional means of judicial cooperation are often deemed too slow and cumbersome for accessing e-evidence, which can be transferred or deleted at the click of a mouse.
- In parallel, voluntary cooperation between law enforcement and US service providers has developed as an alternative path to access e-evidence. This form of cooperation is generally faster than judicial cooperation, but service providers have different approaches regarding the handling of requests for disclosing electronic evidence, and the process lacks transparency and accountability.
- Finally a number of Member States and third countries are working on national solutions that could lead to conflicting obligations for service providers. The current system is patchy and generates legal uncertainty for all parties concerned: for service providers, law enforcement and judicial authorities and also for EU citizens who wonder who can access their data and whether their fundamental rights are sufficiently protected.

The following practical measures to improve cooperation with service providers were identified:

Voluntary cooperation between national authorities and service providers has become the main channel to obtain non-content data, such as information on the subscriber's account. While U.S.-based service providers can provide non-content data to foreign law enforcement, this is currently done in the EU only for service providers based in Ireland.

Measures to improve the situation:

- Establishing single points of contact within Member States to ensure the quality of outgoing requests and build relationships of confidence with providers;
- Streamlining service providers' policies to release the requested data;
- Developing training programmes and exchange of best practice for EU law enforcement and judicial authorities for cooperation with U.S.-based providers;
- Establishing an online information and support portal at EU level to provide support to online investigations.

In addition to the practical measures detailed above the report also examines the potential to introduce legislative measures to improve cross-border access to electronic evidence. Among the measures identified are:

- The issuing of production requests/orders to service providers in another Member State. One of the possible solutions is an EU legal framework enabling authorities to request ("production request") and authorising service providers to respond, or enabling authorities to compel ("production order") a service provider to disclose information about a user, regardless of the location of its headquarters.

[13] https://ec.europa.eu/home-affairs/news/how-can-we-improve-cross-border-access-e-evidence_en

- The direct access to e-evidence. Sometimes finding a service provider to address with a request or order is difficult or impossible and there may be a risk of losing much valuable leads. In such cases, some Member States already make it possible to access the data directly from a device of a suspect or through a computer system. Those investigation techniques have to be considered with caution in view of their potential invasiveness and the risk for fundamental rights and privacy. The conditions and minimum safeguards for direct access in potential cross-border situations could also be set up at EU level.

- Legislative measures beyond the European Union. As the internet is borderless these options for legislative measures could be complemented by agreements with key partner countries or through expanding multilateral treaties, in particular the Council of Europe Budapest Convention on Cybercrime.

The next steps are that The Council will discuss the practical and legislative measures presented by the Commission. The Commission suggests pursuing all practical measures and seeks the views of the Council regarding the necessity and feasibility of legislative measures. If legislative options are supported by the Council, the Commission will launch a public consultation.

While this is to be welcome, it does not yet deal with the practical issues that are met by law enforcement in dealing directly with MSP's. Any solutions are likely to be well into the future and will primarily deal with EU Member States and their relationship within the EU and with US based MSP's.

6 Strategies and possibilities for cooperation

When considering cooperation among law enforcement authorities and multinational service providers (MSPs) there are few aspects to consider how to improve cooperation.

6.1 Requests based on international legal standards

The Council of Europe has prepared a manual on international cooperation on cybercrime and electronic evidence under its GLACY project. It is recommended that the reader of this report considers the content of that manual in conjunction with other references in this report. The issue of MLA is covered in some detail in the manual, which provides information about the legal frameworks, the concept of mutual legal assistance, as well as practical information to support practitioners in preparing effective MLA requests.

The following text is taken form the manual as an introduction to the subject. As this report is dealing with MSP cooperation, it is not proposed to deal with MLA processes in any further detail, as there are other documents that are more relevant.

The multilateral mutual assistance arrangements that exist today may be divided into two categories:

- Firstly, treaties and other arrangements concerning mutual legal assistance in criminal matters exclusively, developing from existing regional or inter-governmental cooperation for example The Council of Europe (hereinafter CoE) The European Union (hereinafter EU) or The Commonwealth,

- Secondly, other treaties covering a particular form of criminality with a mutual legal assistance component, for example the United Nations drugs and crime conventions or the CoE Cybercrime Convention.

The first significant multilateral treaty in the field of mutual assistance was the Council of Europe Convention of 1959 on Mutual Assistance in Criminal Matters and its two Additional Protocols of 1978 and 2001 (hereinafter CoE Convention). The application of the CoE Convention in the European Union was further facilitated in the EU by the EU Convention on Mutual Assistance in Criminal Matters of 2000 and Protocol (hereinafter EU MAC)which in turn formed the basis of the 2nd Additional Protocol to the Council of Europe Convention. The basic provisions of the Council of Europe Convention would set the standard for international mutual legal assistance in other later instruments including the UN drugs and crime conventions and the Scheme on Mutual Legal Assistance in the Commonwealth (hereinafter the Commonwealth Scheme).

6.2 Voluntary Disclosure Model

The voluntary disclosure model is often analysed only from law enforcement perspective and not from MSPs perspective taking into account the MSPs interests, needs and capabilities. There are different levels of engagement, different capabilities and different levels of interest in responding to law enforcement requests by the variety of MSPs. Thus it is difficult to suggest a single approach in order to achieve higher response rates using this voluntary disclosure model. Some providers are very cooperative with law enforcement requests and will have high response rate, others will not respond at all to requests or will scrutinise more depending from the political regime in a particular country. To understand better the business model for a particular platform operated by MSP, it is important to develop direct relationship with each of the major providers. Considering the variety of law enforcement agency within a country that have investigative capabilities and request information it might be difficult for the MSPs to establish the legitimacy of the requests thus it is encouraged to develop single point of contact.

Most MSP's have created online resources to assist law enforcement in making requests for disclosure of information according to the conditions set by the MSP. Each MSP has its own portal and they are not all asking for the same information. This can cause difficulties for LE, however it is incumbent on those making the requests to ensure that they meet the requirements set out by the MSP. Failure to do so will result in no response from the MSP. There now follows, examples of the policies and procedures of selected MSP's. Further information about MSP policies may be found in the Final report of the T-CY Cloud Evidence Group[14] into criminal justice access to electronic evidence in the cloud.

Apple[15]

- Apple publishes/updates guidelines for LE requests for the USA, for Europe/Middle East/India/Africa and for Japan/Asia Pacific. According to these, "nothing will be disclosed without proper legal process…".

In the USA:

- Apple will accept service of subpoenas, search warrants, and court orders for information by email from law enforcement agencies, provided these are transmitted from the official email address of the law enforcement agency concerned

[14] https://rm.coe.int/16806a495e

[15] http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

In the EMEIA region:

- Apple considers a law enforcement information request to be legally valid if it is made in circumstances pertaining to the bona-fide prevention, detection or investigation of offences and will respond appropriately to what it considers to be such legally valid requests.
- Apple Ireland is responsible for the European Union and Switzerland. Apple considers that Irish law applies for data other than content, and US law for content as content is stored in in the US.

Facebook[16]

- With regard to requests from:
- USA authorities, Facebook "disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712."
- International requests, Facebook "disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or Letter Rogatory may be required to compel the disclosure of the contents of an account."
- Facebook Ireland Limited is a subsidiary of Facebook Inc. All users outside of the USA and Canada apparently have a contract with Facebook Ireland Limited.
- Under its "data policy", Facebook
- may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
- Facebook thus may respond to an international request under the domestic legal requirements of the requesting State.
- Facebook maintains a law enforcement portal for requests. https://govtrequests.facebook.com/
- Facebook publishes transparency reports on government requests

Google[17]

- Google publishes guidelines for law enforcement authorities. These guidelines also present information for Google users with regard to how their data can be obtained by criminal justice authorities
- Google can provide user data for Gmail, YouTube, Google Voice and Blogger accounts.
- Google states that it will reply to a request for user data when the request satisfies legal requirements and Google's policies, meaning it is made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law.

[16] www.facebook.com/safety/groups/law/guidelines/

[17] www.google.com/transparencyreport/userdatarequests/legalprocess/

- With regard to requests from US authorities for disclosing information about user data, Google requires a subpoena, court order or search warrant depending on the type of data requested.
- For requests from outside the US, Google may disclose data when the request passes through a Mutual Legal Assistance (MLA) process. Nevertheless, Google mentions that:
- "On a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country".

Microsoft[18]

- Twice a year, Microsoft publishes a report with regard to law enforcement requests for user data.
- Microsoft states that if a Government requests customer data from Microsoft, it needs to follow applicable legal process, meaning it must provide a court warrant or a search warrant for content data, or a subpoena for subscriber information or other non-content data, and that the request must be targeted to a specific account.
- Once receiving a request for data, Microsoft's compliance team will review the demand, verify if it is valid and reject it if considers it is not valid.

Microsoft may reject or challenge a demand for data for a number of reasons, including:

- the request exceeds the authority;
- the requested information is beyond the jurisdiction of the requesting Government or authority;
- the request is not signed or authorized;
- the request is overly broad.

Twitter[19]

- Twitter publishes guidelines for law enforcement authorities. This contains information about available account information, data retention, preservation requests, requests for Twitter account information, emergency requests and mutual legal assistance.
- Data for Periscope and Vine user accounts are also provided by Twitter
- Requests for user account information by law enforcement should be directed to Twitter, Inc. in San Francisco, California, or Twitter International Company in Dublin, Ireland. Twitter responds to valid legal process issued in compliance with applicable law.
- Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request

[18] https://www.microsoft.com/about/csr/transparencyhub/lerr/

[19] https://support.twitter.com/articles/41949#

Yahoo[20]

- Yahoo publishes transparency reports on government requests for data twice per year as well as general "Yahoo Global Principles for Responding to Government Requests". https://transparency.yahoo.com/principles
- Yahoo publishes guidelines for law enforcement authorities requesting compliance with the requirements of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2501 et seq. and 18 U.S.C. § 2703 relating to the disclosure of basic subscriber information, content, and other customer records
- Furthermore, Yahoo required that:
- The legal process specifically identifies the user account that is subject to the request by user ID, email address, screen name or other appropriate identifier.
- All process must be submitted in writing, unless applicable law specifically allows for an oral request.
- All process must be on official letterhead and contain sufficient information to verify that the request has originated with an entity or individual authorized to make such request.

6.3 MSP – Data and Disclosure Provisions

There now follow details of the requirements set by the individual MSP's for dealing with requests for disclosure of information.

Apple

For US requests, Apple, upon a **production order/subpoena** can provide:

- Basic subscriber information (name, physical address, email address and telephone number) related to an iCloud account28, as well as connection logs which are retained up to 30 days
- Basic registration or customer information (name, address, email address and telephone number) related to the registration of an Apple device.
- Customer service records related to devices or services of a customer
- iTunes subscriber information and connection logs with IP addresses
- Subscriber information (including payment card details) for transactions in Apple retail stores or online purchases
- Find My iPhone connection logs
- Media Access Control (MAC) addresses of devices
- IP addresses and other device identifiers related to iOS device activation.

Upon **court order** under 18 U.S.C. §2703(d) or a court order meeting a similar standard:

- iTunes traffic data (transactional records related to purchases or downloads)
- Traffic data related to an email account ("mail logs"), including incoming/outgoing connections and recipient email address
- FaceTime call invitation logs
- **Search warrant** issued upon showing probable cause:
- Specific iTunes content purchased or downloaded

[20] https://transparency.yahoo.com/government-data-requests

- Email or other iCloud content such as photos, documents, calendars, device settings, iMessage, SMS, voicemail etc. iCloud content is encrypted at the location of the server. "Apple retains the encryption keys in its U.S. data centers".
- Data extraction from passcode locked iOS devices (only below iOS 8.0). This can only be performed at Apple California headquarters. Devices need to shipped or brought there.

The guidelines for the **EMEIA** region state that the following information may be available:

- Subscriber information from iCloud including connection logs which are retained for 30 days and may be provided upon a "**legally valid request**"
-
- iCloud mail logs which are retained up to 60 days and may be provided upon a "**legally valid request**"

- Email and other iCloud content and may be provided "only in response to a search warrant issued pursuant to the MLAT process;"

- Device information such as Media Access Control (MAC) address or Unique Device Identifier (UDID) upon a "**legally valid request**"

- Sign-on logs upon a "**legally valid request**".

- Apple accepts service of legally valid LE information requests by email from LE agencies, provided these are transmitted from an official email address of the LE agency. LE officers in EMEIA submitting an information request to Apple should complete a Law Enforcement Information Request template [http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf] transmit it directly from their official LE email address to the mailbox law.enf.emeia@apple.com. This email address is intended solely for submission of law enforcement requests by LE and government agents.

- Unless emergency procedures are used, Apple only discloses content upon a search warrants pursuant to an MLA request or a similar cooperative effort.

- With regard to iTunes, subscriber information and IP connection logs requests need to be sent to the Public Prosecutor in Luxembourg for validation who will forward it to iTunes for response.

Facebook
US Requests

- Upon a production order/subpoena issued in connection with a specific investigation:
- Basic subscriber information (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- Upon a court order:
- Certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber record
- Upon a search warrant or similar issued upon showing probable cause:

- Stored contents of any account, which may include messages, photos, videos, wall posts, and location information.
- Upon National Security Letters:
- Name and length of service

Non US Requests

- Need to be sent to Facebook Ireland and are handled by the Facebook Ireland law enforcement unit. The Facebook conditions and procedures for disclosure to foreign authorities are not very specific.
- It would seem that Facebook Ireland Limited is able to disclose subscriber information [and "certain other records" meaning traffic data] upon request.
- Facebook will not process broad or vague requests.
- All requests must identify requested records with clear identifiable details and include the following:
- The name of the issuing authority,
- Badge/ID number of responsible agent/officer,
- Email address from a law-enforcement domain,
- Direct contact phone number.
- The email address, user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile.
- Requests are to be submitted via the Law Enforcement Online Request System at facebook.com/records

Google
US Requests

Upon a production order/subpoena:

- Subscriber registration information and Sign-in IP addresses and associated time stamps for Gmail and YouTube accounts;
- Subscriber registration information, Sign-in IP addresses and associated time stamps, telephone connection records and billing information for Google Voice accounts;
- Blog registration page and blog owner subscriber information for Blogger
- Upon a **court order**:
- Non-content information and information obtainable with a subpoena, for Gmail accounts;
- Video upload IP address and associated time stamp and information obtainable with a subpoena, for YouTube accounts;
- Forwarding number and information obtainable with a subpoena, for Google Voice accounts;
- IP address and associated time stamp related to a specified blog post, IP address and associated time stamp related to a specified post comment and information obtainable with a subpoena, for Blogger accounts.
- Upon a **search warrant**:

- Email content and information obtainable with a subpoena or court order, for Google accounts;
- Copy of a private video and associated video information, private message content and information obtainable with a subpoena or court order, for YouTube accounts;
- Stored text message content, stored voicemail content and information obtainable with a subpoena or court order, for Google voice accounts;
- Private blog post and comment content and information obtainable with a subpoena or court order, for Blogger accounts.
- The requests for data must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law

Non US Requests

- For requests from outside US, Google can provide the same type of data as the one mentioned above if the request passes through an MLA process.
- However, on a voluntary basis, they may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are:
- Consistent with international norms,
- U.S. law,
- Google's policies and
- The law of the requesting country.

https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

Microsoft

Microsoft can provide:

- Non content data, meaning basic subscriber information (email address, name, address and IP address at the time of registration) or other non-content data (IP connection history, an Xbox Gamertag and credit card or other billing information), upon a production order/subpoena;
- Content data, including content of the emails and documents stored on OneDrive or other cloud offerings such as Office 365 or Azure, upon a court order or a warrant.
- For requests from outside the US, Microsoft can provide basic subscriber information (BSI) and transactional data, directly to upon receipt of a request to their office in the Republic of Ireland.
- For content data, an MLA request is needed.
- Microsoft compliance team reviews the requests for data to ensure the requests are valid, rejects those who are not valid, and only provides data specified in the legal order.
- Microsoft considers that the laws that are applicable for the data of its customers are:
- For data in the US, Microsoft follows the Electronic Communications Privacy Act
- Irish Law and European Union Directives apply to the Hotmail and Outlook.com accounts hosted in Ireland.
- Skype is a wholly owned but independent division of Microsoft, headquartered in and operating according to Luxembourg law.
- https://www.microsoft.com/about/csr/transparencyhub/pppfaq/

Twitter

- Requests for the content of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter.
- Requests for user account information from law enforcement should be directed to Twitter, Inc. in San Francisco, California or Twitter International Company in Dublin, Ireland. Twitter responds to valid legal process issued in compliance with applicable law
- Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request.
- Law enforcement outside US can request content data only by using Mutual Legal Assistance (MLA) requests addressed to US authorities.
- The requests for user information should include the username and URL of the subject Twitter account in question, details about what specific information is requested and its relationship to what investigation, a valid official email address. Requests may be submitted by fax or mail and must be made on law enforcement letterhead.
- Twitter retains different types of information for different time periods, and in accordance with the Terms of Service and Privacy Policy. Some information (e.g., IP logs) may only be stored for a very short period of time. Content deleted by account holders (e.g., Tweets) is generally not available.

Yahoo
US Requests

- Yahoo can provide:
- Content data, upon a search warrant
- Basic subscriber information and transactional data, upon a subpoena or a court order
- Yahoo states that,
- "We provide only that information which we are clearly obligated to provide by the legal process and as allowed by law. We will resist any overly-broad request for our users' information. If we are required to provide information, we produce only limited information to satisfy the demand in order to protect our users' privacy".
- Yahoo will generally accept legal process from a U.S. government agency via email to lawenforcement-request-delivery@yahoo-inc.com
- For requests from outside the USA, Yahoo can provide user data only when the request is submitted through an MLA request. Yahoo does not reply to requests for data addressed directly by non-US law enforcement.
- Yahoo retains different types of information for varied periods of time. In general, user login records for the past year are available in response to legal process. Users can maintain control over the content they store on Yahoo network and may remove, alter, or otherwise modify such content at any time. Such permanently deleted emails are not available in response to legal process.

6.4 Preservation Requests

Apple

- Apple may preserve data upon requests directly received from foreign law enforcement. However, "all iCloud content data stored by Apple is encrypted at the location of the server. When third party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centres." Therefore, preservation requests need to be sent to Apple INC and content can only be obtained via mutual legal assistance requests.
- Furthermore, upon a preservation request for an Apple ID/account email address or physical address or telephone number, Apple will perform a one-time data pull of the existing user data upon and preserve the data for 90 days.

Facebook

- Facebook accepts direct requests for data preservation in connection with official criminal investigations and preserves for 90 days "pending receipt of formal legal process". Requests are to be submitted via the "Law Enforcement Online Request System at facebook.com/records, or by email or post".
- Facebook does not retain data but will try to locate and retrieve data that has not yet been deleted by users upon legal process.

Google

- In practice, Google may preserve data upon requests directly received from foreign law enforcement. A signed letter served by email is required.
- Google will maintain the preservation as long as extensions are sought and Google is told that a Letter of Request LOR is to be sent.

Microsoft

- Microsoft may preserve data upon requests directly received from foreign law enforcement. Microsoft requires a signed letter served by fax.
- Microsoft will preserve records initially for 180 days and maintain the preservation for 90-day periods thereafter as long as timely extensions are sought and Microsoft is told that a Letter of request (LOR) is to be sent
- Microsoft will not communicate law enforcement whether an account identifier is valid. The above mentioned information does not apply to requests for cloud data.

Twitter

- Twitter accepts requests from law enforcement to preserve records, preserving a temporary snapshot of the relevant account records for 90 days pending service of valid legal process.
- Preservation requests, in accordance with applicable law, should be signed by the requesting official, include the @username and URL of the subject Twitter profile (e.g., @safety and https://twitter.com/safety), have a valid return official email address, and be sent on law enforcement letterhead. https://support.twitter.com/articles/41949#

Yahoo

- Yahoo preserves user data, to the extent it is available, for 90 days upon receipt of a valid preservation request from a government agency issued in accordance with applicable law.
- Preservation requests from non-US law enforcement are accepted https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

6.5 Emergency Requests

All companies have specific policies to deal with emergency requests and the criteria are very much the same for each company, with prevention of death and serious injury being common, but not exclusive criteria.

Apple

- For requests from the EMEIA region, Apple considers a request to be an emergency request if there is a "bona-fide and serious threat to:
- 1) the life/safety of individual(s);
- 2) the security of a State;
- 3) commit substantial damage to critical infrastructure or installations."
- For emergency requests in the EMEIA region the following template is to be used: http://www.apple.com/legal/privacy/le-emergencyrequest.pdf
- Before disclosing customer data, Apple will contact the supervisor of the requesting officer for confirmation of the legitimacy of the request. A requesting officer may also call a hotline to notify Apple of an emergency request.
- Apple will inform the customer within 90 days of the request for data.

Facebook

- In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records.

Google

- With regard to emergency procedures, Google states that:
- "Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm".

Microsoft

- In limited circumstances, Microsoft discloses information to criminal law enforcement agencies when:

- The disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Microsoft considers emergency requests from law enforcement agencies around the world.
- Those requests must be in writing on official letterhead, and
- signed by a law enforcement authority.
- The request must contain a summary of the emergency, along with an explanation of how the information sought will assist law enforcement in addressing the emergency.
- Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the disclosure is limited to the data that they believe would enable LE to address the emergency. Some of the most common emergency requests involve suicide threats and kidnappings.

Twitter

- Twitter states that when receiving request for data in an emergency situation
- it evaluates emergency disclosure requests on a case-by-case basis in compliance with relevant law (e.g., 18 U.S.C. § 2702(b)(8) and Section 8 Irish Data Protection 1988 and 2003). If they receive information that provides them with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, they may provide information necessary to prevent that harm, if they have it.

Yahoo

- Consistent with the emergency disclosure provisions in ECPA (18 U.S.C. § 2702), Yahoo make disclosures to government officials in instances where they have been provided sufficient information to conclude that disclosure without delay is necessary to prevent imminent danger of death or serious physical injury to any person. All emergency disclosure requests should be submitted in writing using our Emergency Disclosure Form. Yahoo will, in its sole discretion, determine whether the circumstances warrant disclosure, utilizing the information provided on the Emergency Disclosure Form. Consistent with our commitment to protecting our users' privacy and discretion allowed under ECPA, we reserve the right to only share information that we believe is necessary to avert an emergency situation.

6.6 Customer Notification

All the above providers WILL notify their customers of any request for their data UNLESS:

- When prohibited by the law (pursuant to 18 U.S.C. § 2705(b) (ECPA)).
- In emergency cases;
- Where notice could result in danger;
- Where notice could be counterproductive.

Other than legal prohibition, the decision to disclose is made by the companies.

This is an important consideration for criminal justice authorities and one of which they must be aware in advance of making any request to MSP's. There are situations where potentially, the personal details of the requesting person could be released to the person who is the subject of the request. In cases involving terrorism or organised crime groups, this could place the individual at risk.

6.7 Quality of Relationship with MSPs

The usual complaint by law enforcement authorities is the low level of response they get to requests sent to MSPs. From MSPs perspective is that from these countries they are getting very limited number of requests and thus the quality of the received ones are not corresponding with the international legal standards and thus were not responded to.

Law enforcement need to focus more on developing direct relationships with service providers, encourage service providers to assist countries to provide training on how to prepare quality requests; which requisites need to be included in a request form and also learn when a request will not be dealt with. When such direct cooperation model is established and learned how to prepare quality requests this will directly reflect on the response rate and increase the responses.

Relationships with MSPs on regular basis are a must and are the only solution to positive outcomes when it comes to voluntary disclosure method.

6.8 Information Requested

There are few major reasons to disqualify a request sent by law enforcement:

- Information requested by law enforcement is in violation of freedom of speech or human rights: in such cases the MSPs will reject the request and not respond. Countries requesting information must comply with privacy principle and have good legislation in place in relation to privacy and human rights. If a request comes from law enforcement from a country with controversial experience or legislation in these areas the chances are very high that the multinational service provider might not respond to the request.

- Quality of the request: law enforcement from these countries have limited experience in applying the voluntary disclosure model and send very few requests for information on annual bases. This lack of experience and maturity in dealing with MSPs might reflect on the quality of the request and miss some of the obligatory information.

- MSPs need to understand the context in which a crime is taking place. Thus it is necessary to provide as much information as possible about a case, so the MSP understands what you are requesting the information for. Ex. It is not sufficient to provide only the article of the criminal code under which you are investigating an individual. It is necessary to describe the case stating the facts. This information will help the MSPs on one hand to understand the context and on the other to provide you with the exact information you need.

- Vague requests: very often a request will not ask for concrete information. This poses challenges for MSPs to determine why and what information is needed and will not respond to a request.

- Requests sent in national language: all requests should be sent translated in English language.

One of the major issues is that not all requests for information will be responded by MSPs if direct communication channels are used. Considered will be only complete requests, which contain all the necessary requisites as described in the MSPs policies (such information is

available online in the law enforcement resource section of every MSPs website), are asking only for basic subscriber information and contain an element of threat or fast reaction. This should not be confused with emergency requests for which the service providers have a distinct procedure.

7 Conclusions

Lawful access to data by law enforcement is a fundamental requirement for criminal justice systems to operate effectively and fairly. Access to such data may protect victims of crime and give them access to justice, as well as providing evidence of innocence or guilt of individuals. The challenges offered by the data they need being outside the jurisdiction, is not new, however the extent to which electronic evidence is needed has expanded beyond all recognition in recent years.

Direct requests to MSP's have both advantages and disadvantages for the administration of justice. On the positive side, direct requests enable rapid requests for data to be made. What happens next, is totally in the hands of the individual MSP. This is a rather unusual situation for law enforcement as there is no compulsion, other than goodwill for the MSP to respond. At the national level, law enforcement is used to making lawful applications for access to data under national legislation, where court or other legal orders will have legal weight and often give a deadline for the release of the data.

There are clearly issues with the quality of some submissions to MSP, even though most use a template format for completion by the law enforcement agency. This is in part because there is no requirement by the MSP for the request to be submitted by a Designated Point of Contact (POC), such as the designated 24/7 POC for parties to the BCC, or POC's of the G8 countries network. Similarly, there is no evidence that countries require all requests to be sent via such POC's, through which an element of quality control and suitability of the requests could be made.

The decision by MSP's not to respond to many requests, or give a reason for refusal of requests, often leaves investigators, victims, witnesses and suspects "in limbo", with no idea if or when a response may be received. This leads to unnecessary delays in investigations and an ill-informed opinion of some MSP's by the authorities.

Other than emergency requests, there is no prioritisation list for requests, in place to assist requesting and requested parties to better evaluate each request and provide a trusted method of establish the importance of requests. An agreed timetable of responses would also be beneficial.

Perhaps one of the main issues that lead to misunderstanding between parties is that there is no direct discussion or explanation of each parties concerns with the process. At the national level, there are examples of how discussion can ameliorate many of the problems. One example is the United Kingdom, where similar challenges were identified as long ago as 1986. Government, Law enforcement and the Internet Industry met to discuss how the lawful access to data could be achieved most effectively. Interestingly the model in place at that time was that of voluntary disclosure under provisions of the UK Data Protection Legislation. As with the current international situation, the decision to release data was made by the ISP. A discussion group was created which later became known as the Internet Crime Forum. This led to an improvement in the quality of requests, better decision making by ISP's, development of dedicated POC's on each side and ultimately joint representation to government to introduce legislation to control lawful access to data with appropriate

safeguards. Creating a small working group to develop the recommendations from this report, the report of the Cloud Evidence Group and the provisional recommendations of the European Commission, will lead to the opportunity to create a more satisfactory environment in which lawful access to data may be more effectively managed and safeguards ensured.

The current situation, although a genuine attempt to deal with what has become a serious issue for criminal justice process, has created its own problems. The sheer scale of the level of requests is beginning to impact adversely on the business of MSP's and they are incurring significant costs in dealing with direct requests. Improvements in the future administration of requests require action on the part of both requesting and requested parties.

The only real prospect for improvement is for the parties (or representative groups) to discuss the issues and try to understand how the current difficulties impact on the businesses of the MSP's on one hand and the effective administration of justice on the other. It is clear, from national solutions that have been provided, that there is room for improvement and some of these may provide a baseline for discussion. Agreement from all MSP's and all LE may be challenging, however as with all solutions, the benefits are often not seen until positive action has been taken. Inertia is not an option, in this case. Ultimately, the MSP community could simply insist that all requests are made through the MLAT procedures and this is not a desired outcome, for the administration of justice.

The following, non-exhaustive list identifies some of the issues that may be included for discussion:

- Broad and Strategic Cooperation
- Legislation
- Procedures for Legally Binding Requests
- Designated Contact Points
- Training for LE and MSP's
- Technical Resources
- Authority for Requests
- Verification of Source of Request
- Standard Request Format
- Specificity and Accuracy of Requests
- Prioritisation of requests based on agreed criteria
- Responses to requests
- Appropriateness of requests
- Confidentiality of data
- Disclosure of existence of requests
- Coordination among Law Enforcement Agencies
- Cross border service of national production orders
- Criminal compliance programmes (Audit)
- Costs
- Public awareness and crime prevention

The overarching strategy is to identify initiatives/topics of mutual importance to law enforcement and MSP's and seek joint approach in finding solutions or improving the situation. Such initiatives will improve the relationships between MSP's and law enforcement and will increase the level of trust which will have direct implications on the direct cooperation model. Efforts should be made to obtain mature cooperation models with individual providers rather than standard forms for requesting information.