

The logo for GLACY+ is displayed in a large, white, sans-serif font against a dark blue background. To the left of the text, there is a partial view of a globe showing green continents and blue oceans, with some faint, illegible text overlaid on it.

Global Action on Cybercrime Extended  
Action Globale sur la Cybercriminalité Élargie

Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe

**EU/COE Joint Project on Global Action on Cybercrime**

# **Cooperation with the Private Sector in the Fight against Cybercrime**

**Joint ECOWAS-Council of Europe Regional Conference**

**Abuja, Nigeria – 11 September 2017**

**T. GEORGE-MARIA TYENDEZWA, CFE**  
*Assistant Director | Head,  
Cybercrime Prosecution Unit,  
Department of Public Prosecutions  
Federal Ministry of Justice,  
Abuja, Nigeria*



## **Some questions:**

**How many here have smart phones?**

**How many are connected to the Internet now?**

**How many have a Hotmail, Outlook, Gmail or Yahoo account?**

**Who knows where their data is being stored?**



## **Microsoft Corporation (2014)**

**1 million servers in  
100+ datacenters in 40 countries**

### **Emails**

**Content data will where possible be in your region  
Subscriber data will be in the USA**



# Google Datacenters

## Americas

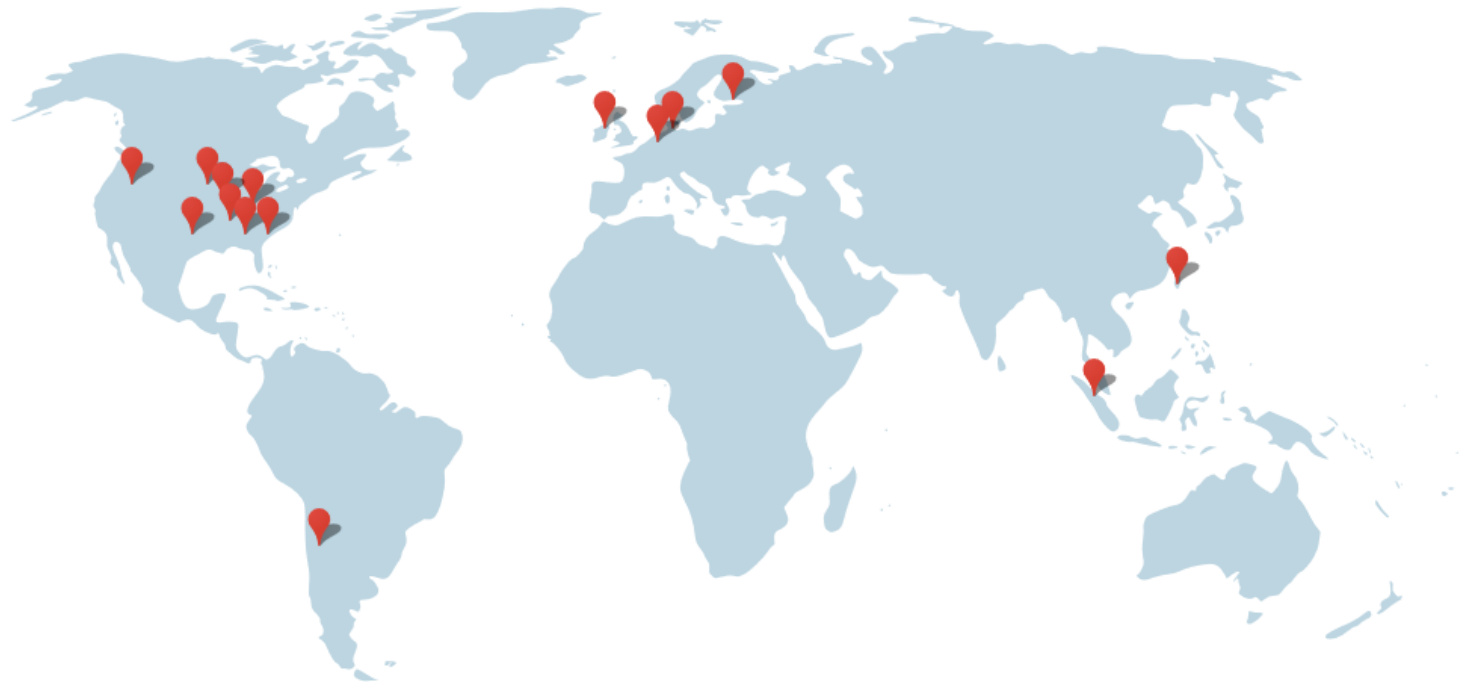
- Berkeley County, South Carolina
- Council Bluffs, Iowa
- Douglas County, Georgia
- Jackson County, Alabama
- Lenoir, North Carolina
- Mayes County, Oklahoma
- Montgomery County, Tennessee
- Quilicura, Chile
- The Dalles, Oregon

## Asia

- Changhua County, Taiwan
- Singapore

## Europe

- Dublin, Ireland
- Eemshaven, Netherlands
- Hamina, Finland
- St Ghislain, Belgium





# Apple

Apple will accept service of **legally valid** law enforcement information requests by email from law enforcement agencies, provided these are transmitted from the **official email address** of the law enforcement agency concerned. Law enforcement officers in EMEIA submitting an information request to Apple should **complete a Law Enforcement Information Request template** and transmit it **directly from their official law enforcement email address to the mailbox [law.enf.emeia@apple.com](mailto:law.enf.emeia@apple.com)**. This email address is intended solely for submission of law enforcement **requests by law enforcement 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**.





## Facebook



Facebook Requests from regions other than the USA or Canada 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 request.



# Facebook Law Enforcement Guidelines

FACEBOOK CONFIDENTIAL AND PROPRIETARY

© Facebook, Inc. 2010. All Rights Reserved.



# facebook

## Facebook Law Enforcement Guidelines

This guide describes the procedures law enforcement authorities should follow to request data from Facebook, Inc. and its corporate affiliates (“Facebook”) and explains the types of data that may be requested.

This guide is **CONFIDENTIAL** and intended for **law enforcement use only**. Please do not redistribute it without the express written permission of Facebook.

As described in the Facebook Statement of Rights and Responsibilities, Facebook “strives to create a global community with consistent standards for everyone but also strives to respect local laws”. (see <http://www.facebook.com/terms.php>). With regard to law enforcement inquiries in particular, Facebook will respond to requests if the company believes in good faith that compliance is required by local law and relates to users from the jurisdiction. (see <http://www.facebook.com/policy.php>)

Facebook’s services continuously change and the company reserves the right to change any of the policies described in these guidelines without notice. Contact Facebook at [subpoena@fb.com](mailto:subpoena@fb.com) to request the latest version of these guidelines.



# Twitter LEA Request Form

## Law Enforcement Request

Please fill out all the fields below so we can review your report

---

Tell us about yourself

- I am an authorized law enforcement representative (e.g., police officer, federal agent).
- I am an authorized government representative (e.g., district attorney, minister).
- None of the above.

Type of request or report

How can we help?

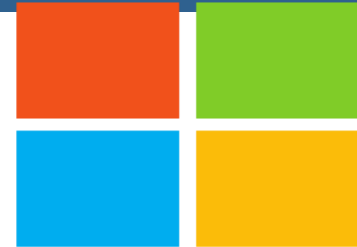
- Request for account information
  - Non-emergency information request
  - Emergency disclosure request
- Report potentially illegal content
- Report other violations
- Other inquiries

Emergency Disclosure Request





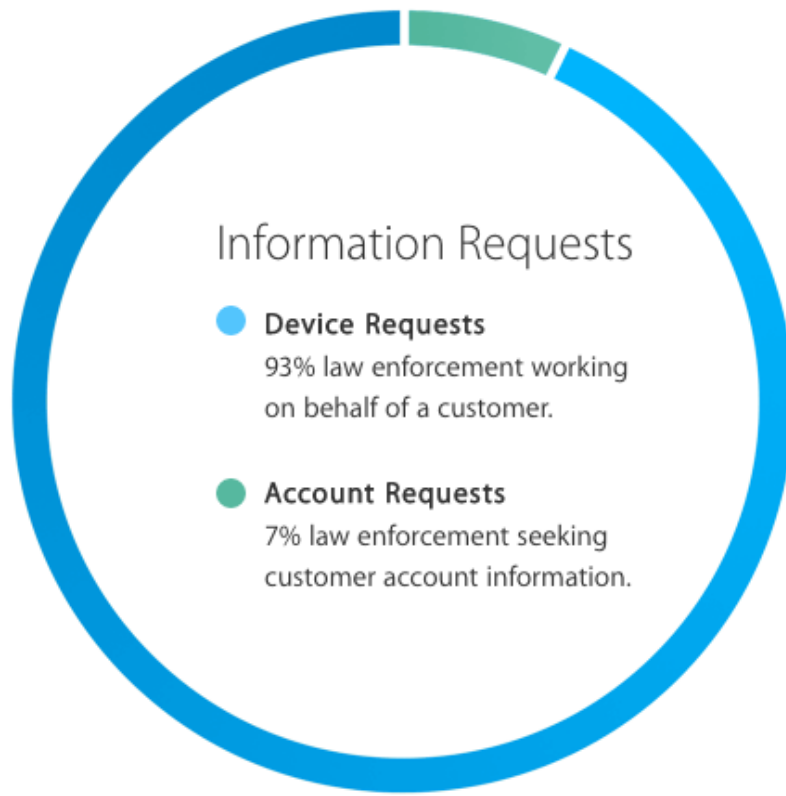
## Microsoft



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 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.

# Types of Requests Received by Apple



## Information Requests

- **Device Requests**  
93% law enforcement working on behalf of a customer.
- **Account Requests**  
7% law enforcement seeking customer account information.

## Device Requests

The vast majority of the requests Apple receives from law enforcement come from an agency working on behalf of a customer who has requested assistance locating a stolen device. We encourage any customer who suspects their device is stolen to contact their respective law enforcement agency.

## Account Requests

Responding to an Account Request most often involves providing information about a customer's iTunes or iCloud account. Only a small fraction of requests from law enforcement seek content such as email, photos, and other content stored on customers' iCloud or iTunes accounts.



- ❖ **Data can be moved (for admin reasons) at the speed of light between countries**
- ❖ **Backed up in more than one country**
- ❖ **Content and subscriber data stored in different countries**
- ❖ **One message may be split between different countries**
- ❖ **Service providers do not know where it is**

**Where To Send Your Request?**



## **USA Allows direct requests to Commercial Service Providers (will see in later module) BUT:**

Survey of direct requests by Budapest Convention Parties for Subscriber Data to **Apple, Facebook, Microsoft, Twitter and Yahoo** in 2014

**189,289 Requests**

**128,048 Responses with data (68%)**



**32% unresponsive requests can be due to:**

- **No data available;**
- **Improperly completed request;**
- **Inaccurate details provided;**
- **Unable to verify legal authority for request.**

**(But 'No. of Requests' also includes those resubmitted)**



# Considerations in Cooperating with Foreign Service Providers

- Volatility of policies
- Location, territoriality and jurisdiction
- US vs European providers
- Direct & emergency requests
- Different requirements for different types of data



# Volatility of Policies

- Service provider policies lack foreseeability
- Policies can be and are changed unilaterally without prior notice
- Policies are applied differently for different Parties to Budapest Convention



# Location, Territoriality & Jurisdiction

- Conditions for access to subscriber information determined by:
  - location of service provider and regulations governing such service provider
  - whether requesting law enforcement authority has jurisdiction over offence
- Content data in US is not always voluntarily disclosed – often requires formal request to US Government







## Direct preservation & emergency requests

- US service providers accept requests for preservation made directly by foreign authorities
- US service providers have procedures for accepting emergency requests



## Different requirements for different types of data

- US Service Providers require different levels of safeguards to disclose different kinds of data
- Access to subscriber information may be accepted on a production order while a court order may be required to access content information

# E.g. Google Inc.



- Upon production order/sub poena:

- Subscriber registration information and sign-in IP addresses and associated time stamps for Gmail/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

# E.g. Google Inc.

- Upon court order:
  - Non-content information for Gmail accounts
  - Video upload IP addresses and associated time stamp and information obtainable with a subpoena for YouTube accounts
  - Forwarding number and information obtainable with subpoena for Google Voice account
  - IP address and associated time stamp related to a specified blog post, IP address and associated time stamp for blogger accounts



# E.g. Google Inc.

- Upon search warrant:

- Email content and information obtainable with a subpoena or court order for Google's accounts
- Copy of private video and associated video information, private message content for YouTube accounts
- Stored text message content, stored voicemail content for Google voice accounts
- Private blog posts and comment content for Blogger accounts





# **Legal Basis for Direct Cooperation with Private Service Providers**



# **Article 18 – Production Order**





## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



3 For the purpose of this article, the term “subscriber information” means 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.



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its **competent authorities** to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## Competent authorities

- May be:
  - law enforcement official; or
  - judicial authority; or
  - prosecutor



- May vary depending on type of computer data involved
- BUT NOTE:
- **Central Authorities** – are defined by law and may be different from **Competent Authorities**



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a **person in its territory** to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## Person in its territory

- Person must be resident in territory
- Not apply to persons who are not present in territory
- Person includes service provider
- Requirement: of person presence in territory; not data in territory



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to **submit specified computer data** in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## Specified computer data

- PO used in **individual cases** usually concerning **specific persons**
- Not authorize issuance of orders requiring disclosure of indiscriminate [ANY] amounts of data
- Less intrusive than search and seizure







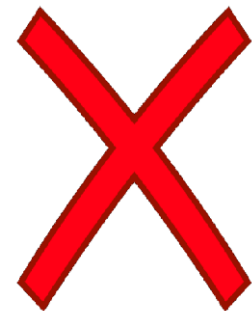
## Specified computer data

Examples:

A. Order production of email address associated with a particular name



B. Order production of ALL communications during last three years associated with a particular name





## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's **possession or control**, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

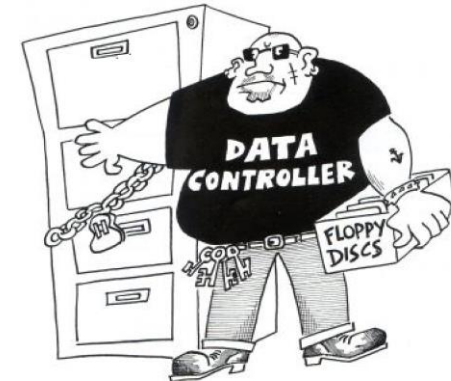


## Possession or Control

- Physical possession of data concerned within territory

OR

- Free control of production of data concerned (“constructive possession”) whether or not within territory
- Not include mere technical ability to access remotely stored data not within legitimate control



*Google  
Ireland  
Preserve/  
Disclose*

*But*

*Location  
could be  
Finland*



## International Aspects

### Extend power Outside Territory

- Article 18.1.a. – “possession or control” covers
  - **Physical possession** of data **within** ordering party’s territory
  - **Free control over data **outside** ordering party’s territory**



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is **stored in a computer system or a computer-data storage medium**; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## Stored in computer system

- Production of stored (existing) data, either in:
  1. Computer system
  2. Computer data storage medium
- Does not impose obligation for service providers to retain data – but retention necessary for power to be effective





## Stored in computer system

- **Not** production of:
  - **content data** related to **future communications** (interception)
  - **traffic data** related to **future communications** (real-time collection)
- Location of data **irrelevant**; extends to:
  - Cloud data
  - Other remotely stored data



## International Aspects

- Storage of data in another territory does not prevent application of Article 18
- Covers storage facility **outside** territory
- Covers cloud data stored **outside** territory





## International Aspects

- Production order is the only domestic power that includes extra-territorial powers
- Recognized by Cloud Evidence Group and in T-CY Guidance Note on Article 18

16 September 2016  
Strasbourg, France



T-CY (2016)5  
Provisional

**Cybercrime Convention Committee (T-CY)**

**Criminal justice access to  
electronic evidence in the cloud:**

**Recommendations for consideration by the T-CY**



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b **service provider** offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## Service Provider

- Includes any private or public entity that:
  - **provides ability to communicate** by means of computer system
  - **processes/stores computer data** on behalf of such entities



## Service Provider

- Irrelevant whether its users form closed group or whether providers offer services to public
- Irrelevant whether services provided free of charge or for fee





## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

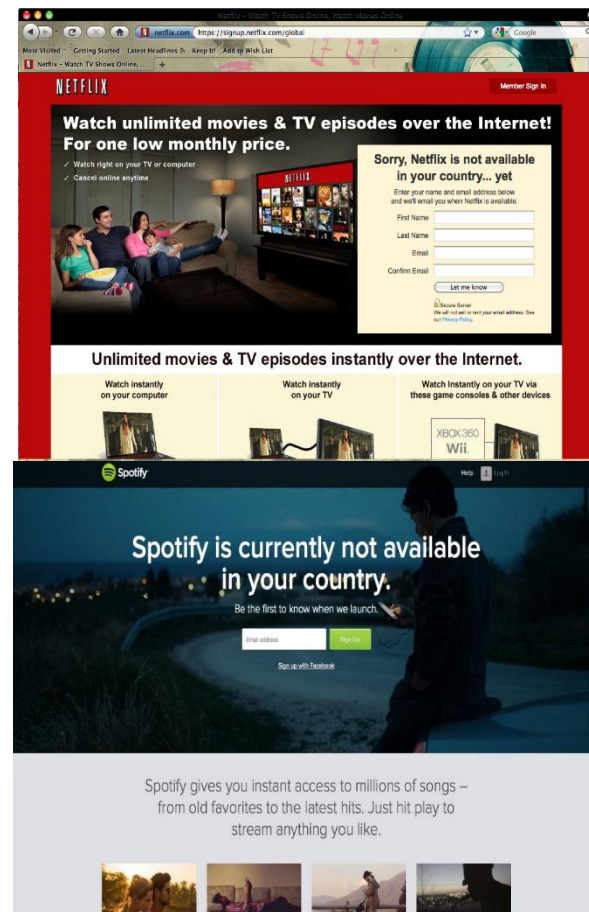
a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider **offering its services in the territory of the Party** to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

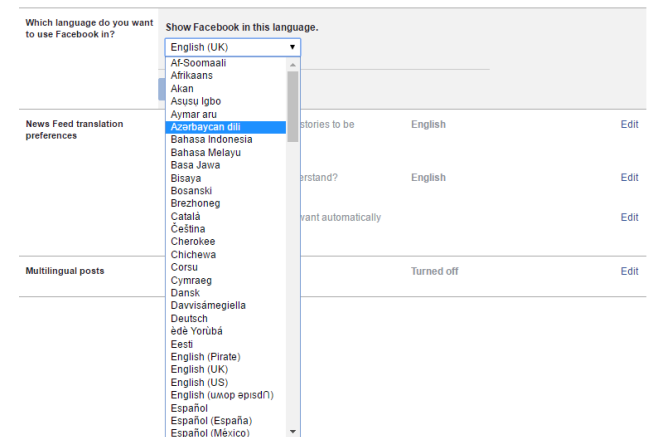
## Offering services in the territory of a Party

- Service provider offers services in the territory of a Party when:
  - service provider **enables persons to subscribe to its services** (e.g. does not block service); OR
  - **makes use of the subscriber information** in the course of its activities, OR



## Offering services in the territory of a Party

- Service provider offers services in the territory of a Party when:
  - orients its activities toward such subscribers (e.g. local advertising or ads in local language), OR
  - interacts with subscribers in the Territory.
- Service provider can offer services in a territory even if its TLD refers to another jurisdiction. [.uk .pk .tr .com .net]







## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit **subscriber information** relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.





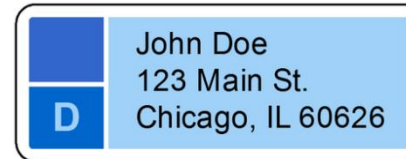
## Subscriber Information

- Information in form of computer data/**any other form** relating to subscribers of its services (other than content data and traffic data)
- Most requested in investigations
- Usually held by private sector service providers
- Obtained through production orders

## Subscriber Information

Enables establishment of:

- Type of communication services used
- Period of service
- Subscriber's:
  - Identity
  - Postal address
  - Telephone
  - Billing information
  - Payment information
- Other information on site of installation of communication equipment





## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:


a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information **relating to such services** in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## Relating to such services

- PO issued for purpose of obtaining subscriber information relating to services offered in ordering Party's territory
- Does not apply to information relating to services offered solely outside ordering Party's territory.



The screenshot displays a web portal interface with a navigation bar at the top containing tabs for "Subscriber", "Packages", "Statements", and "Usage". The main content area is titled "Primary Contact" and features a profile icon on the left. The contact information is organized into several rows of input fields:

- Company: [Empty field]
- First Name: Dwight | MI: [Empty field] | Last: Colton
- Address 1: P.O. Box 567
- Address 2: [Empty field]
- City: Selma | State: RI | Zip: 97538
- Home Phone: 0- | Work Phone: 0-
- Cell Phone: 0- | Fax: 0-

On the right side of the form, there are two buttons: "Change Login" (with a person icon) and "Billing Info" (with a document icon).



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

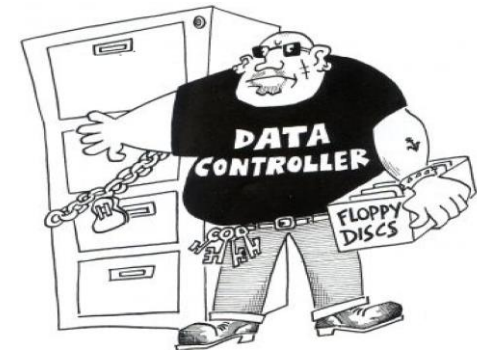
b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that **service provider's possession or control.**

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## Possession or Control

- Includes:
  - subscriber information in the service provider's physical possession
  - local or remotely stored subscriber information under the service provider's control
- Does not include:
  - mere technical ability to access remotely stored data not within legitimate control of service provider





## International Aspects

- Article 18.1.b. – “possession or control” covers
  - Physical possession of subscriber information in service provider’s physical possession
  - **Remotely stored subscriber information under service provider’s control**



**IF**

**The criminal justice authority has jurisdiction over the offence in line with Article 22 Budapest Convention;**

**AND IF**

**The service provider is in possession or control of subscriber information**

**AND IF**

**Article 18.1.a**  
**The person is in the territory of the Party. For example, the service provider is registered as a provider of electronic communication services, or servers or parts of its infrastructure are located in the Party;**

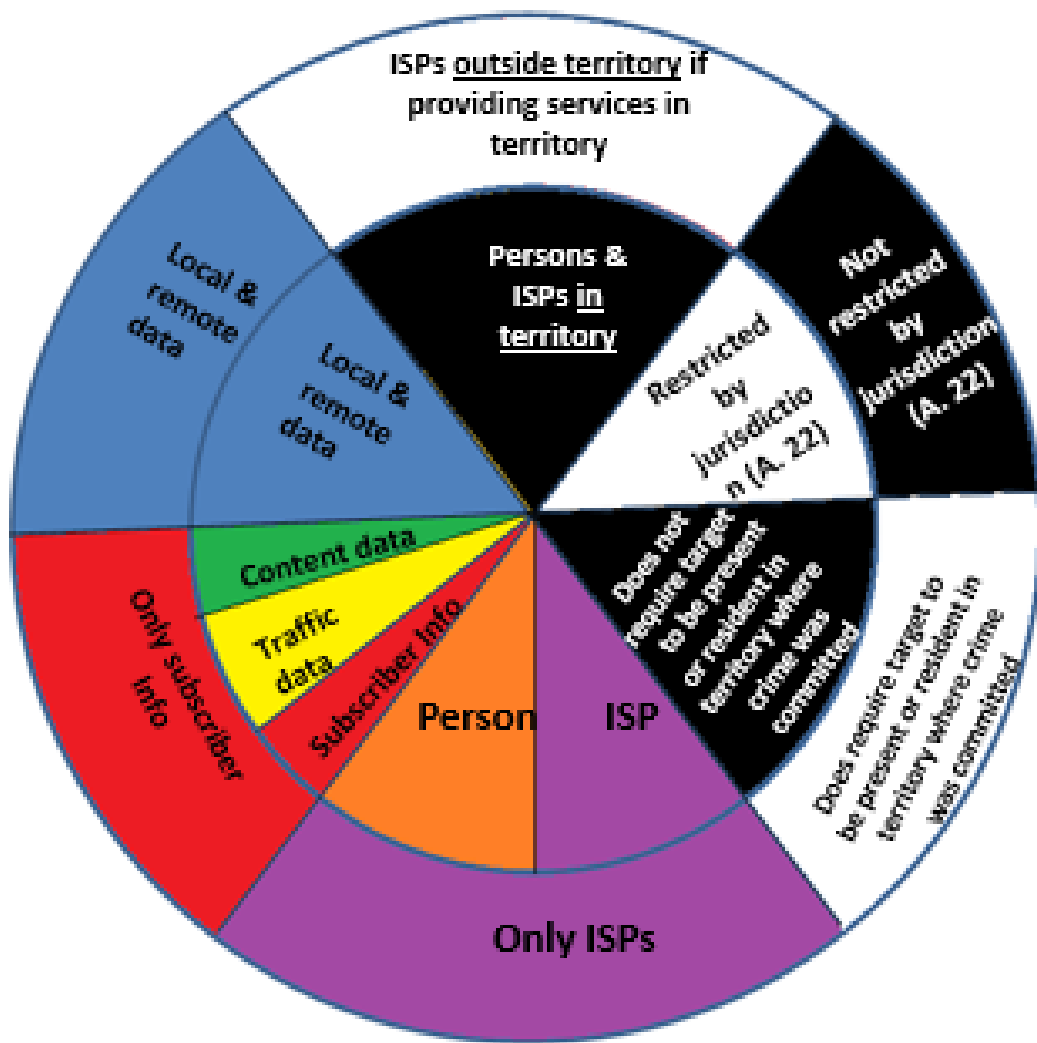
**OR**

**Article 18.1.b**  
**The service provider is “offering a service in the territory of the Party”, when, for example:**  
**– the service provider enables persons in the territory of the Party to subscribe to its services, AND**  
**– orients its activities at subscribers, or makes use of subscriber information in the course of its activities, or interacts with subscribers in the Party;**

**AND IF**

**the subscriber information to be produced is relating to services of a provider offered in the territory of the Party, even if those services are provided via a technical geographic domain referring to another jurisdiction**





Inner Circle: Article 18.1.a.  
Outer Circle: Article 18.1.b.



## Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be **subject to Articles 14 and 15.**



## Conditions & Safeguards

- Depending on type of data (e.g. content data, traffic data or subscriber information), different:
  - competent authority
  - terms
  - Safeguards
- However, independent authority must order production



## Conditions & Safeguards

- Proportionality principle – parties may not allow use of production orders in minor cases
- Confidentiality of requests/orders
- May exclude privileged data or information



# **Article 32 – Trans-border access to stored computer data with consent or where publically available**



## **Trans-border access to data – Article 32**

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.



A Party may, **without the authorisation of another Party**:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.



## Without authorization of the other Party

- Does not require mutual assistance
- Does not require notification to other Party
- Does not exclude notification and Parties may notify each other if they deem it appropriate





## Trans-border access to data – Article 32

A Party may, without the authorisation of another Party:

- a **access publicly available (open source) stored computer data, regardless of where the data is located geographically; or**
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

## Publically available data

- Law enforcement can access publically available (open source) data without authorization
- If portion of website is closed to public then it is not considered publically available
- Geographical location of data not relevant





## Trans-border access to data – Article 32

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, **stored computer data located in another Party**, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.



## **Stored computer data located in another Party**

- Article 32b may be used where it is known where data is located
- Article 32b may not be used if:
  - Data is not stored in another Party
  - It is uncertain where data is located
  - Data is stored domestically



## Trans-border access to data – Article 32

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the **lawful and voluntary consent** of the person who has the lawful authority to disclose the data to the Party through that computer system.



## Lawful & voluntary consent

- Person providing consent must not be forced or deceived
- Minors or persons with mental or other conditions may not be able to give consent under domestic law



## Lawful & voluntary consent

- Most parties require explicit consent for cooperation in criminal investigations
- Agreement to general terms and conditions of online service may not suffice as consent



## Trans-border access to data – Article 32

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the **person who has the lawful authority to disclose the data** to the Party through that computer system.





## Person who has lawful authority to disclose data

- Depends on circumstances, laws and regulations
- Example: You may provide access to an email that is stored abroad to a law enforcement official
- Service providers usually:
  - can't consent validly to disclosure of user data
  - are holders of user data but do not own/control it



- **Production order (Article 18)**

- Mandatory cooperation
- Consent of subject not necessary
- May be used to access computer data & subscriber information within and outside territory of Party
- Only domestic power that can be applied to entities outside the country

- **Trans-border access (Article 32b)**

- Voluntary cooperation
- Valid and lawful Consent necessary
- May not be used to access data domestically



## Questions

*Thank You for your attention.*

**T. George-Maria TYENDEZWA, CFE**

*Assistant Director | Head,  
Cybercrime Prosecution Unit,*

Federal Ministry of Justice, Abuja,

E: [terlumun.tyendezwa@justice.gov.ng](mailto:terlumun.tyendezwa@justice.gov.ng)

Alt: [tyendezwaTG@cybersecurity.gov.ng](mailto:tyendezwaTG@cybersecurity.gov.ng)

W: [www.justice.gov.ng](http://www.justice.gov.ng)