Provisional version 3 May 2016
Strasbourg, France

T-CY (2016)2
Provisional

Cybercrime Convention Committee (T-CY)

Criminal justice access to data in the cloud:

Cooperation with "foreign" service providers

Background paper

prepared by the T-CY Cloud Evidence Group

www.coe.int/TCY

Contents

Contact
Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

1 Purpose of this report

The Cybercrime Convention Committee (T-CY), at its 12th plenary (2-3 December 2014), established a working group to explore solutions to access for criminal justice purposes to evidence in the cloud, including through mutual legal assistance ("Cloud Evidence Group").[1] The Cloud Evidence Group is to submit a report to the T-CY with options and recommendations for further action by December 2016.

In 2015, the T-CY Cloud Evidence Group, following a discussion paper summarizing the challenges of criminal justice access to data in the cloud (published in May 2015 and discussed at the Octopus Conference in June 2015), held a hearing for providers on 30 November 2015 which focused on the direct cooperation by criminal justice authorities with service providers in foreign jurisdictions:

Often a prosecution or police authority (a "law enforcement authority") of a Party to the Budapest Convention requests a service provider in another jurisdiction for data in relation to a specific criminal investigation. Typically, subscriber information is sought from multinational service providers with their headquarters in the USA ("US service providers"). Some of them have subsidiaries in Europe or elsewhere.

Transparency reports published by US service providers indicate that they respond positively to about 60% of such requests "on a voluntary basis".

Article 18 Budapest Convention covers "production orders" and Article 18.1.b specifically the production of subscriber information by a service provider "offering its services on the territory of the Party":

> 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 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 a 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.

The Explanatory Report (paragraph 171) to the Budapest Convention indicates Article 18 was also intended to cover situations of voluntary cooperation:

> 171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

The purpose of the present background paper is to provide a snapshot[2] of policies and practices of some major US service providers regarding their "voluntary" disclosure of information to law enforcement authorities in foreign jurisdictions,[3] and thus to facilitate discussion of future options regarding criminal justice access to electronic evidence in the cloud.

[1] Document T-CY(2014)16: Transborder Access to data and jurisdiction: Options for further action by the T-CY (report of the Transborder Group adopted by the 12th Plenary of the T-CY, December 2014).
[2] Note: Provider policies and practices change frequently, including while the present report was prepared.
[3] The scope of Article 18 will be covered in more detail in a separate report.

2 Direct cooperation with foreign providers

2.1 The scale of direct requests to US service providers by Parties to the Budapest Convention

In recent years, many service providers with their Headquarters in the USA began to publish "transparency reports" on requests for data received from governments for law enforcement purposes. Voluntary disclosure of "customer records" – and of contents in emergency situations – is possible under US law, that is, the Electronic Communications Privacy Act.[4]

Figures for 2014 related to six of these providers (Apple, Facebook, Google, Microsoft, Twitter and Yahoo) show that 45 out of 48 Parties to the Budapest Convention[5]) had sent requests to one or more of them. Parties (including the USA) had sent about 190,000 requests in total. Parties other than the USA had sent some 109,000 requests to these six US service providers and in about 65,000 cases (60% of the requests) received at least some of the data requested. Provisional data for 2015 show similar patterns.

The data requested and disclosed in almost all the cases was for user or account information, that is, primarily subscriber information. Contents was rarely requested or disclosed.

These figures do not yet cover direct requests for removal of contents or device information[6] or requests directly sent to many other providers.

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2014[7]		
Parties	**Received**	**Disclosure**	**%**
Albania	24	7	29%
Armenia	11	2	18%
Australia	6 438	4,236	66%
Austria	246	73	30%
Azerbaijan	-	-	
Belgium	1,804	1,316	73%
Bosnia and Herzegovina	13	8	62%
Bulgaria	5	3	60%
Canada	850	477	56%
Croatia	45	34	76%
Cyprus	38	21	55%

[4] 18 U.S. Code §2702 https://www.law.cornell.edu/uscode/text/18/2702
[5] The exceptions were Azerbaijan, Mauritius and "The former Yugoslav Republic of Macedonia". Provisional data for 2015 indicate the Azerbaijan and "The former Yugoslav Republic of Macedonia" also sent requests.
[6] For example, in 2014, Parties other than the USA sent some 27,000 requests to Apple covering several hundred thousand devices.
[7] Source: Transparency reports
Apple http://www.apple.com/privacy/transparency-reports/
Facebook https://govtrequests.facebook.com/about/#
Google https://www.google.com/transparencyreport/
Microsoft https://www.microsoft.com/about/csr/transparencyhub/
Twitter https://transparency.twitter.com/
Yahoo https://transparency.yahoo.com/government-data-requests

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2014[7]		
Parties	**Received**	**Disclosure**	**%**
Czech Republic	333	204	61%
Denmark	362	225	62%
Dominican Republic	54	30	56%
Estonia	35	19	54%
Finland	144	102	71%
France	21,772	12,863	59%
Georgia	1	0	0%
Germany	25,519	13,801	54%
Hungary	345	159	46%
Iceland	3	2	67%
Italy	9,365	4,620	49%
Japan	1,617	1,010	62%
Latvia	2	2	100%
Lichtenstein	5	1	20%
Lithuania	49	28	57%
Luxembourg	153	117	76%
Malta	377	197	52%
Mauritius	-	-	
Moldova	13	7	54%
Montenegro	7	1	14%
Netherlands	1,099	856	78%
Norway	363	238	65%
Panama	88	68	77%
Poland	1,747	550	31%
Portugal	2,223	1,356	61%
Romania	80	40	50%
Serbia	16	9	56%
Slovakia	107	36	34%
Slovenia	11	6	55%
Spain	4,462	2,391	54%
Sri Lanka	1	-	0%
Switzerland	462	266	58%
"The former Yugoslav Republic of Macedonia"	-	-	
Turkey	8,405	5,625	67%
Ukraine	8	2	25%
United Kingdom	20,127	13,894	69%
USA	80,703	63,147	78%
Total excluding USA	**108,829**	**64,901**	**60%**
Total including USA	**189,532**	**128,048**	**68%**

Figures show very uneven patterns:

- France, Germany and the UK each sent more than 20,000 requests directly to the six providers, while Bulgaria, Iceland, Latvia, Lichtenstein, Georgia, Montenegro, Sri Lanka and Ukraine sent less than 10 and Azerbaijan, Mauritius and "The former Yugoslav Republic of Macedonia" none at all in 2014. Provisional data for 2015 indicate the Azerbaijan and "The former Yugoslav Republic of Macedonia" also sent requests.

- The level of partial or complete disclosure of data varies between the six providers: Microsoft is the most responsive provider (78% for Parties other than the USA), followed by Google (54%), Facebook (48%) and Apple (38%) while Yahoo (34%) and Twitter (21%) are the least responsive. Yahoo rejects most requests not for "data not available" but for other reasons.[8]

- The six providers cooperate in a very inconsistent manner with different Parties. In terms of disclosure rates, for example:

  - Google cooperates above average with Finland (83%), Netherlands (81%) and Japan (79%) but below average with Poland (29%) and Slovakia (8%) and not all with Hungary (0%) or Turkey (0%).
  - Microsoft on the other hands cooperates rather well with Hungary (83%) and Turkey (76%).
  - Facebook also responds well to Hungary (83%) and Turkey (66%), but less to Poland (29%), Portugal (38%) and Spain (37%).
  - Yahoo cooperates with Australia (51%) but responds not at all to Netherlands, Norway, Portugal and Switzerland.
  - Microsoft on the other hand cooperates very well with Netherlands (83%), Norway (82%), Portugal (85%) and Switzerland (74%).
  - Twitter cooperates above average with Australia (58%), Japan (36%) and Norway (50%) but not at all with Turkey (0%) and below average with France (11%), Germany (16%) or Spain (12%).

- The differences in the level of responses to Parties is also reflected in the Google data related to content removal where Google/You Tube in 2014 removed content following 49% of the more than 14,000 requests from Parties other than the USA. The response to requests from France (76%), Italy (73%) contrasts with the response to Turkey (35%) or Australia (33%).

- However, there is another important observation regarding request for removal of contents by Google/You Tube: Whether or not the request is backed up by a court order seems to be of little relevance. Requests with court order lead to removal in 53% of the cases against 49% of the total average.

[8] "Yahoo may have possessed data responsive to the Government Data Request, but none was produced because of a defect or other problem with the Government Data Request (e.g., the government agency sought information outside its jurisdiction or the request only sought data that could not be lawfully obtained with the legal process provided). This category also includes Government Data Requests that were withdrawn after being received by Yahoo. We carefully review Government Data Requests for legal sufficiency and interpret them narrowly in an effort to produce the least amount of data necessary to comply with the request."
https://transparency.yahoo.com/faq/index.htm#list_item_4

- The six providers reviewed in the present report do not provide the complete picture. Requests are also sent to many others. For example, Snapchat[9] – in the period January to June 2015 – received 82 requests from some of the Parties other than the USA (Australia, Canada, Czech Republic, Denmark, France, Norway, Spain and UK) but only responded to emergency requests (in 73% of emergency requests some data was produced).

2.2 Policies and procedures by providers

2.2.1 LEA guidelines

2.2.1.1 Example Apple

Apple publishes and updates guidelines for law enforcement requests for the USA, for Europe/Middle East/India/Africa and for Japan/Asia Pacific.[10] 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.[11]

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.[12]

In the Japan/APAC region:

> Apple considers a law enforcement legal process document to be valid if it is a Cooperation Letter, a Notice of Obtaining Evidence, subpoena, court order, search and seizure warrant, Australian Telecommunications Act of 1979 Authorization Letter or the local equivalent of these valid legal requests. The type of document required by Apple may vary from country to country and depends on the information sought.[13]

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.

According to Apple's Privacy Guidelines[14]

> International Users
> All the information you provide may be transferred or accessed by entities around the world as described in this Privacy Policy. Apple abides by the "safe harbor" frameworks set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information

[9] https://www.snapchat.com/transparency/
[10] http://www.apple.com/privacy/government-information-requests/
[11] http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf
[12] http://images.apple.com/privacy/docs/legal-process-guidelines-emeia.pdf
[13] http://images.apple.com/privacy/docs/legal-process-guidelines-apac.pdf
[14] http://www.apple.com/legal/privacy/en-ww/ This site – accessed on 3 March 2016 – still referred to the Safe Harbour Programme which by that time had however been discontinued. The site was "last updated 17 September 2014".

> collected by organizations in the European Economic Area and Switzerland. Learn more about the U.S. Department of Commerce Safe Harbor Program.
> Please note that personal information, including the information provided when using iCloud, regarding individuals who reside in a member state of the European Economic Area (EEA) and Switzerland is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA and Switzerland when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc.

2.2.1.2 Example Facebook

Facebook is publishing operational guidelines for law enforcement authorities.[15]

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.[16]

Under its "data policy"[17], 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. Facebook publishes transparency reports on government requests.[18]

2.2.1.3 Example Google

Google is publishing 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.[19]

Google can provide user data for Gmail, YouTube, Google Voice and Blogger accounts.

[15] https://www.facebook.com/safety/groups/law/guidelines/
[16] https://en.wikipedia.org/wiki/Facebook
[17] https://govtrequests.facebook.com/
[18] https://www.facebook.com/about/privacy/other
[19] https://www.google.com/transparencyreport/userdatarequests/legalprocess/

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.

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[20]:

> 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.

2.2.1.4 Example Microsoft

Twice a year, Microsoft publishes a report with regard to law enforcement requests for user data[21].

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.

2.2.1.5 Example Twitter

Twitter is publishing guidelines for law enforcement authorities[22]. 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[23] and Vine[24] 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.

[20] https://www.google.com/transparencyreport/userdatarequests/legalprocess/
[21] https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/
[22] https://support.twitter.com/articles/41949#
[23] https://www.periscope.tv/
[24] https://vine.co/

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.

2.2.1.6 Example Yahoo

Yahoo is publishing transparency reports on government requests for data twice per year[25] as well as general "Yahoo Global Principles for Responding to Government Requests".[26]

Yahoo had been publishing guidelines for law enforcement authorities[27] 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.

2.2.2 Types of data available and procedures and conditions for disclosure

2.2.2.1 Example Apple

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

- Basic subscriber information (name, physical address, email address and telephone number) related to an iCloud account[28], 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

[25] https://transparency.yahoo.com/
[26] https://transparency.yahoo.com/principles
[27] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm However, by the end of March 2016, this site was not accessible anymore. The following is a link to link to a "Yahoo! Compliance Guide For Law Enforcement:
http://r.search.yahoo.com/_ylt=AwrBTzwtAflWGCYA5vpXNyoA;_ylu=X3oDMTEydTYzYW4wBGNvbG8DYmYxBHBvcwMyBHZ0aWQDQTAxOTZfMQRzZWMDc3I-/RV=2/RE=1459188141/RO=10/RU=https%3a%2f%2fwww.eff.org%2ffiles%2ffilenode%2fsocial_network%2fyahoo_sn_leg-doj.pdf/RK=0/RS=6PiFEwB8arANWnhrQwZeY5adxk8-
[28] Apple requires an Apple ID/email account or subscriber information in the form of full name, phone number or physical address to identify the account.

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
- 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".

In terms of procedures:

> 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 [http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf] transmit it directly from their official law enforcement email address to the mailbox 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.

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.

However, for the Japan/APAC region:

> When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, iTunes subscriber information

and connection logs with IP addresses can be obtained with the appropriate legal process document for the requester's country.[29]

2.2.2.2 Example Facebook

For requests from the USA, Facebook can provide,

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 records

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

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.

> All requests must identify requested records with particularity and include the following:
> - The name of the issuing authority, badge/ID number of responsible agent, email address from a law-enforcement domain, and 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

[29] http://images.apple.com/privacy/docs/legal-process-guidelines-apac.pdf

2.2.2.3 Example Google

For requests from an USA authority, Google can provide the following:

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.

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, 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.[30]

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

2.2.2.4 Example Microsoft

For requests from the US, 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.

Example of Microsoft providing "basic subscriber information"[31]

Below is an example of exactly what law enforcement receives when Microsoft produces basic subscriber information, using a test account registered by a Microsoft employee. Although we changed the name and are masking the extension for security reasons, all other information is exactly what Microsoft produces to law enforcement.

Field	Value
Login	First.Last@xxxxxxx.com
PUID	0006BFFDA0FF8810
First Name	First
Last Name	Last
State	Washington
Zip	98052
Country	US
Timezone	America/Los_Angeles
Registered from IP	65.55.161.10
Date Registered {Pacific}	10/24/2007 1:05:18 PM
Gender	M
Last Login IP	64.4.1.11

The PUID in the above table stands for "Personal User ID," which is a unique alpha-numeric code generated for each registered Microsoft account.

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.

Microsoft considers that the laws that are applicable for the data of its customers are:

- For the data stored in US, Microsoft follows the Electronic Communication Privacy Act (ECPA).

[31] https://www.microsoft.com/about/csr/transparencyhub/pppfaq/

- 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.

2.2.2.5 Example 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.

2.2.2.6 Example Yahoo

For requests from the US, 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[32].

Yahoo will generally accept legal process from a U.S. government agency via email to lawenforcement-request-delivery@yahoo-inc.com.

[32] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

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

2.2.3 Preservation requests

2.2.3.1 Example 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.

2.2.3.2 Example 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.

2.2.3.3 Example 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.

2.2.3.4 Example Microsoft

In practice, 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.

2.2.3.5 Example 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.[33]

2.2.3.6 Example Yahoo

> We preserve 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.[34]

Preservation requests from non-US law enforcement are accepted.

2.2.4 Emergency procedures

2.2.4.1 Example 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:

> It is Apple's policy to notify a customer when we receive an emergency request from law enforcement requesting customer account information after 90 days of receipt of the request.

2.2.4.2 Example 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.

[33] https://support.twitter.com/articles/41949#
[34] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

2.2.4.3 Example 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[35].

2.2.4.4 Example Microsoft

Microsoft has a program to disclose information in response to imminent emergency requests.

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 we believe would enable law enforcement to address the emergency. Some of the most common emergency requests involve suicide threats and kidnappings[36].

2.2.4.5 Example Twitter

Twitter may disclose account information to law enforcement in response to a valid emergency disclosure request.

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 we receive information that provides us with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it[37].

2.2.4.6 Example Yahoo

> Consistent with the emergency disclosure provisions in ECPA (18 U.S.C. § 2702), we make disclosures to government officials in instances where we 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,

[35] https://www.google.com/transparencyreport/userdatarequests/legalprocess/
[36] https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/
[37] https://support.twitter.com/articles/41949#

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.[38]

2.2.5 Customer notification

2.2.5.1 Example Apple

Apple will notify its customers when their personal information is being sought in a legally valid law enforcement information request except where it reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.
Apple will provide delayed notice for emergency requests except where Apple reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice. Apple will provide delayed notice for requests after expiration of a non-disclosure period specified in a court order except where Apple reasonably considers that to do so would likely pervert the course of justice or prejudice the administration of justice.

The template for emergency requests[39] notes:

It is Apple's policy to notify a customer when we receive an emergency request from law enforcement requesting customer account information after 90 days of receipt of the request.

2.2.5.2 Example Facebook

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will provide delayed notice upon expiry of a specific non-disclosure period in a court order and where we have a belief, in good faith, that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Police officials who believe that notification would jeopardise an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.[40]

2.2.5.3 Example Google

When receiving a request for data, Google will notify the user via email before any information is disclosed. Exceptions:

- A statute, court order or other legal limitation;
- An exceptional circumstances involving danger of death or serious physical injury to any person;
- A reason to believe that the notice wouldn't go to the actual account holder, for instance, if an account has been hijacked.

[38] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm

[39] http://www.apple.com/legal/privacy/le-emergencyrequest.pdf

[40] https://www.facebook.com/safety/groups/law/guidelines/

2.2.5.4 Example Microsoft

When receiving a request for data, Microsoft will notify the user via email before any information is disclosed. Exceptions:

- When prohibited by the law;
- In emergency cases;
- Where notice could result in danger;
- Where notice could be counterproductive.

Even in these cases, Microsoft will provide delayed notice to users upon expiration of the valid and applicable non-disclosure order, unless considers that this notification will result in danger for individuals or will be counterproductive.

2.2.5.5 Example Twitter

> Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account compromises). We may also provide post-notice to affected users when prior notice is prohibited.[41]

2.2.5.6 Example Yahoo

> Our policy is to explicitly notify our users about third-party requests for their information prior to disclosure, and thereby provide them with an opportunity to challenge requests for their data. In some cases, we may be prohibited by law from doing so, such as when we receive a non-disclosure order pursuant to 18 U.S.C. § 2705(b). Additionally, in exceptional circumstances, such as imminent threats of physical harm to a person, we may elect to provide delayed notice. When the circumstance that prevented us from providing notice prior to disclosure is removed, e.g., the non-disclosure order expired or the threat has passed, we take steps to inform the affected user(s) that data was disclosed[42].

2.3 Law enforcement/service provider agreements

In several Parties, the authorities have concluded agreements or made arrangements to improve cooperation with US service providers. This includes the use of agree upon templates for requests, procedures to be followed and the establishment of single points of contact. Examples are France and Portugal.

In Parties where such arrangements are in place, larger numbers of requests are send and information received. Both, criminal justice authorities and service providers underline that such good practices can make a difference.[43]

[41] https://support.twitter.com/articles/41949#
[42] https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm
[43] See also the Guidelines on law enforcement/ISP cooperation developed in 2008.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba

3 Issues[44]

The voluntary disclosure of subscriber information by US service providers is most valuable to criminal justice authorities in Parties to the Budapest Convention. Nevertheless, a number of issues and concerns have been raised.

3.1 Volatility of provider policies

Provider policies are volatile and lack foreseeability for law enforcement[45] as well as customers. Service providers may change their policies unilaterally at any time and without prior notice to law enforcement.[46]

Adding to this, policies and practices not only differ widely between providers but also with respect to different Parties to the Budapest Convention. One provider may respond to many requests from one country but to none or a few requests only from another country, while the practices of another provider may be exactly the opposite.

Overall, provider policies and practices are volatile and unpredictable which is problematic from a rule of law perspective.

3.2 Location

The problems of location, territoriality and jurisdiction have been described in the discussion paper on "Criminal justice access to data in the cloud: challenges".[47]

With respect to the cooperation between US service providers and law enforcement authorities of other Parties, it would seem that with regard to requests for subscriber information, the actual location of the data or servers is of limited relevance. Conditions for access to subscriber information seem to be determined by (a) the location of the service provider and the regulations that govern the service provider, and (b) whether the requesting law enforcement authority has jurisdiction over the offence investigated. Under certain conditions, US service providers tend to disclose subscriber

[44] The issues have been raised by law enforcement authorities and service providers in the hearing on 30 November 2015. As Chatham House Rules had been agreed upon, they are not attributed to a specific provider or law enforcement authority.

[45] For example, see the Italian situation in 2006-2008 (with Google, Microsoft and Yahoo's branches all based in Milan):
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2625
Microsoft Italia was the first to provide – without a rogatory letter upon a request from the Italian Public Prosecutor – subscriber information, not only referring to *hotmail.it* accounts but also to *hotmail.com* email accounts.
At first Google Italia talked about the need of a MLA for any request. Then, after the Italian Google case, they changed their policy and began providing subscriber information directly on the condition that there was an order from the Italian Public Prosecutor (and not only an order from the Italian Judicial Police). Nevertheless, if an IP address (logged by the Google electronic systems with regard to an e-mail *@gmail.com*) was not related to an Italian server, this company considered itself unable to communicate it to the Italian Judicial Authority.
Yahoo! Italia on the other hand required a rogatory letter only in some cases, having a software called *Yahoo! Account Management Tool* which returned also content data if requested (specifically the data of e-mail boxes @*yahoo.it* and/or @*yahoo.com*) but only from users who had chosen – at the moment of their registration - the Italian law (according to a principle called "*Net Citinzenship*"). Yahoo! Italia was also able to provide an e-mail interception to the Italian Judicial Authority (without a MLA request).
Yahoo!, while directly disclosing also content data to the Italian Judicial Authority, in the same years did not disclose anything to the Belgian Judicial Authorities (see the Belgian Yahoo! case).

[46] Apple: Legal Process Guidelines version 29 September 2015: "Nothing within these Guidelines is meant to create any enforceable rights against Apple and Apple's policies may be updated or changed in the future without further notice to law enforcement."

[47] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

information to law enforcement authorities in countries where they are offering a service as foreseen in Article 18.1.b Budapest Convention.

European providers seem to be bound by rules of territoriality, including the location of data. The hearing held on 30 November 2015[48] suggests that for European providers this is a major obstacle to business.

With regard to content data, US providers are unclear. In some instances, they may argue that content is stored in the US and thus voluntary disclosure is not possible (unless in emergency situations). In other instances, where data may be stored in Europe, they still require a mutual legal assistance request to be sent to the US Government.

3.3 "US" versus "European" and other providers

US service providers are able to disclose subscriber and traffic data directly and voluntarily to foreign law enforcement authorities upon request. Content may also be provided in emergency situations. This is permitted under US law (Electronic Communications Privacy Act). [49]

It would seem that European providers are not disclosing data directly to foreign authorities and only respond to orders received via domestic authorities following mutual legal assistance requests.

The reasons are not entirely clear. While providers of "electronic communication services" in Europe are normally under a strict regime regarding the disclosure of traffic data, providers of "Internet society services" should in principle be able to disclose subscriber information under legitimate, vital or public interest considerations.

The consequence is a one-way flow of data from US service providers to the law enforcement authorities of Parties in Europe and other regions, while service providers in Europe or other Parties do not disclose data directly and voluntarily to the authorities in the US or other Parties.

Increasingly, US service provider are represented within the European Union – for example through subsidiaries in Ireland – and are thus subject to European Union law, including data protection regulations. This may restrict possibilities for direct and voluntary transborder cooperation in the future.

On the other hand, one may ask why what is possible for US service providers located or represented within the European Union – namely the voluntary disclosure of subscriber information or, in emergency situations also of other data – would not be possible for European service providers.

3.4 Domestic legal basis for obtaining subscriber information

US service providers – when receiving requests for data from foreign law enforcement authorities – consider the domestic legal framework of the requesting authority, including whether the requesting authority would have the power to request a certain type of data from a service provider at the domestic level.

As documented in the T-CY report on rules for obtaining subscriber information[50], conditions for access to such data vary between the Parties. In some, police officers and in others prosecutors can request

[48] http://www.coe.int/en/web/cybercrime/hearing
[49] 18 U.S. Code §2702 https://www.law.cornell.edu/uscode/text/18/2702

the production of subscriber information while in some others court orders are required. In the latter case, service providers may not respond to a request from a police or prosecution authority.

In some Parties, a distinction is made between subscriber information (and other data) held by telecommunication service providers and information held by Internet society service providers. Given the convergence of different types of services and service providers, this distinction is increasingly problematic in practice.

The lack of harmonization of rules for obtaining subscriber information in Parties to the Budapest Convention complicates matters for providers that are willing to cooperate.

A further issue is the admissibility of information received voluntarily from a service provider abroad as evidence in criminal proceedings. In some Parties it is admissible, in others it is not.

This suggests that a clear legal basis for obtaining subscriber information in domestic law, preferably harmonized in Parties, would facilitate more systematic cooperation with providers in foreign jurisdictions and use of information received in criminal proceedings.

3.5 Direct preservation requests

US service providers accept requests for preservation directly received from foreign authorities. However, the fact that often there is no follow up through mutual legal assistance is of concern to them.

European providers do not accept preservation requests received directly from law enforcement authorities in other jurisdictions.

3.6 Emergency requests

US service providers foresee procedures for cooperation in emergency situations, including the disclosure of contents.

In some Parties, specific procedures have been agreed upon, including centralized systems with contact points. In these Parties, the experience seems to be positive overall, although cooperation with some providers is considered not always predictable or reliable even in emergency situations.

It would seem that while US service providers do cooperate in principle in emergency situations, European providers do not disclose subscriber information or other data directly to foreign authorities, even in emergency situations.

3.7 Customer notification

The notification of a customer of a request from a foreign authority by US service providers is considered a major concern by law enforcement authorities.

While confidentiality requirements may be enforced in domestic legal requests, this is less the case in situations of voluntary cooperation with a foreign provider.

[50] T-CY (2014)17
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

Customer notification: Example provided by a prosecutor of a Party to the Budapest Convention (November 2015)

1. On someone's [Social Media Account], we see that someone writes in the name of ISIS that [CITY] will be attacked on [DATE]
2. We also found these postings on the [Social Media Account]
3. [Social Media Provider] disclosed subscriber and login information based on our emergency request. So far so good.
4. We could see that there's a [Webmail] email connected to that [Social Media Account].
5. So, in order to have more information, I did a similar request to [Webmail provider].
6. They sent me their new policy where they write clearly that also for imminent physical threat procedures they have the right to advise their client.
7. So we asked for more clarification... "ONE QUESTION ABOUT THE [Webmail Provider] DISCLOSURE POLICY: WHAT INFORMATION ABOUT THE REQUESTER WOULD YOU PROVIDE TO THE ACCOUNT HOLDER? WOULD IT BE SOMETHING RELATIVELY GENERAL LIKE "THE AUTHORITIES OF [COUNTRY]" OR WOULD YOU DISCLOSE THE ACTUAL NAME AND EMAIL ADDRESS OF THE PERSON WHO SIGNED THE EMERGENCY DISCLOSURE REQUEST. WE WOULD LIKE TO KNOW THIS AS THIS MAY MEAN THAT A POTENTIAL TERRORIST MAY RECEIVE PERSONAL INFORMATION OF A LAW ENFORCEMENT OFFICER.
8. They called me back, telling me that they understand the situation, but they cannot guarantee that after 90 days my contact information won't be given to the client.

3.8 Data protection

The more US providers are represented in Europe, the more they will be subject to European data protection rules.

European and international data protection instruments cover transborder data transfers either from one private sector entity to another private sector entity or from one competent criminal justice authority to another criminal justice authority.

The "asymmetric" transfer of data from a law enforcement authority of one jurisdiction to a private sector entity in another jurisdiction in another State is permitted under specific conditions.[51]

However, for the "asymmetric" voluntary disclosure of data – such as subscriber information – from a private sector service provider to a law enforcement authority in another State, clear rules permitting such transfers seem not available.

Providers need to assess themselves whether the condition of lawfulness is met, whether it is in the public interest or whether it is in the legitimate interest of the provider as the data controller to disclose data. Providers may run the risk of being held liable. A clearer framework for private to public transborder disclosure of data would be required, including conditions and safeguards. This would help service providers avoid situations of conflicting legal obligations.

[51] Article 14 of Framework Decision 2008/977/JHA http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN and Article 36 aa of the draft future EU Directive on data protection in the criminal justice sector http://statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft-final-compromise-15174-15.pdf

Example: Facebook Ireland audit by Irish Data Protection Commissioner 2011/2012

In 2011 and 2012, Facebook Ireland was audited by the Irish Data Protection Commissioner, including with respect to disclosure to foreign authorities.[52]

The legal basis allowing Facebook to disclose data to criminal justice authorities is Article 8 of the Irish Data Protection Act which states that "any restrictions in this Act on the processing of personal data do not apply", among other things, if the processing is required for crime prevention and criminal justice purposes. Sections 8(b) and (d) are considered particularly relevant:

8.-Any restrictions in this Act on the processing of personal data do not apply if the processing is-

> (b) required for the purpose of preventing, detecting or investigating offences, apprehending
> or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application
> of those restrictions would be likely to prejudice any of the matters aforesaid,
>
> (d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property,

The Facebook Ireland law enforcement unit thus assesses whether these conditions are met before responding to a request. "Each request is examined by virtue of the legal authority of the requesting law enforcement agency and the nature of the personal data sought." [53]

An important feature of the procedure is that Facebook Ireland cooperates with designated single points of contact (SPOC) within law enforcement authorities. "The advantage of this approach is that it minimises the risk of inappropriate requests for data". [54]

Furthermore, "the legal basis cited in each request is examined for compatibility with applicable law and if any doubt arises further advice is sought from in-house or external legal counsel." [55]

The procedure of Facebook was audited in 2011[56] and 2012. The 2011 audit report refers to five requests selected at random from the UK, Italy, Belgium, Germany and Italy to examine whether the criteria of Sections 8(b) and 8(d) of the Irish Data Protection Act had been fulfilled. In 2012, a further five examples were examined (from France, Germany, Italy, Portugal, UK and Ireland). Facebook reject some and granted other requests. The sample only covered EU member States.

[52] See Section 3.7 (page 98 ff) and appendix 5 in the report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
See Section 2.7 (page 34 ff) in the report of 2012
https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm
[53] Page 99 of the Audit report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[54] Page 99 of the Audit report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[55] Page 99 of the Audit report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[56] See Section 3.7 (page 98 ff) and appendix 5 in the report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
See Section 2.7 (page 34 ff) in the report of 2012
https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm

The Facebook procedures and practices regarding disclosure to foreign authorities were considered in line with Irish data protection law by the auditors and Sections 8(b) and (d) were considered a sufficient legal basis.

This is interesting given that States within the EU or other Parties to Convention 108 normally have similar provisions in their domestic data protection laws. If these were interpreted in a similar way, service providers in these countries would also be able to disclose data in a similar way to foreign authorities.

For content, an MLA request must be sent to the Irish authorities:

"should the law enforcement agency require content information from FB-I, we will require that we be served with a legally compelling request under Irish law. The Gardaí (Irish Police) will be required to produce a search warrant or similar coercive document. Non-Irish search warrants will only be respected by FB-I if they are enforceable as a matter of Irish law. This will require that any such orders be domesticated by way of application to the Department of Justice pursuant to the Criminal Justice (Mutual Assistance) Act 2008."[57]

3.9 Lawful requests versus voluntary cooperation

A lawful order by a police, prosecutor or judge served on a physical or legal person is binding and can be enforced on the territory of the authority.

However, under the current practice of direct transborder cooperation, US service providers consider their cooperation as "voluntary".

The current practice thus combines a lawful, coercive request with voluntary cooperation.

US service providers seem to prefer to keep this practice.

From a law enforcement perspective this appears to be problematic as service providers determine whether or not to cooperate, evaluate the legality of the request, or check dual criminality and other conditions. This applies not only to requests for data received from police, but also prosecutors and courts; and in the end the requests are not enforceable.[58] The fact that service providers appear to be above the law is problematic from a rule of law perspective.

4 Conclusions

The European Court of Human Rights, in the case of K. U. v. Finland[59] in December 2008, underlined the obligation of States to protect the rights of individuals, including through efficient criminal law measures. In its analysis, the Court referred to the procedural law provisions of the Budapest Convention on Cybercrime, including in particular the production of subscriber information under Article 18. It also referred to the need for efficient cooperation between service providers and law

[57] Page 99 of the Audit report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[58] See in this connection the final judgement by the Belgian Court of Cassation confirming that Yahoo! is obliged to produce data upon a lawful request for data in Belgium.
http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f
[59] http://hudoc.echr.coe.int/eng#{"dmdocnumber":["843777"],"itemid":["001-89964"]}

enforcement authorities as proposed in Guidelines adopted by the Council of Europe Octopus Conference in April 2008.[60]

Thus, cooperation between service providers and law enforcement authorities is essential for crime prevention and criminal justice, for the strengthening of the rule of law and for the protection of human rights.

US service providers often cooperate directly transborder with law enforcement authorities of other Parties to the Budapest Convention and disclose in particular subscriber information. In many ways, this is in line with Article 18.1.b Budapest Convention.

In this context, a service provider having possession or control of the data cooperates with a law enforcement authority having jurisdiction over a specific offence which is being investigated. The actual location of data and servers is of limited relevance.

Parties to the Budapest Convention – other than the USA – send more than 100,000 requests per year to major US service providers and receive (at least partial) data in about 60% of the cases.

This practice of US service providers is most valuable for crime prevention and criminal justice.

At the same time, this practice is volatile and unpredictable and raises a number of data protection and rule of law concerns.

European and most other non-US service providers normally do not cooperate directly with foreign law enforcement authorities but seem to be more strictly governed by rules of territoriality (location of controller and location of data).

The distinction between electronic communication service providers and Internet society service providers adds further complexity in a context where the same provider may offer different types of services.[61]

In conclusion, a common disclosure policy for all types of providers would be desirable.

Continuation of the dialogue with service providers is necessary. Regular meetings of the T-CY with service providers, the establishment of an online tool with up-to-date provider policies and procedures as well as information on relevant legislation and criminal justice authorities responsible in Parties, and common templates for requests for subscriber information may help improve current practices with respect to Parties to the Budapest Convention.

However, it will not only be necessary to improve current practices, but to establish clear domestic and international legal frameworks to ensure greater legal certainty for law enforcement and industry and to remove obstacles for businesses.[62] Such a solution may be constructed around Article 18 Budapest Convention and/or provisions in an Additional Protocol to the Convention.

[60] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba
[61] It is understood that the European Union may revise the E-Privacy Directive 2002/58/EC. Proposals include removal of the distinction between electronic communication service providers and Internet society service providers. https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data
[62] This was also the conclusion the hearing for service providers held on 30 November 2015 http://www.coe.int/en/web/cybercrime/hearing

5 Appendix

5.1 Direct requests by Parties to major providers in 2014

2014	All providers			Requests share/all parties	Google and You Tube			Microsoft and Skype			Yahoo		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Albania	24	7	29%	0,01%	2	-	0%	-	-	0%	1	-	0%
Armenia	11	2	18%	0,01%	1	-	0%	4	1	25%	1	-	0%
Australia	6 438	4 236	66%	3,40%	1 711	1 014	59%	2 332	1 845	79%	769	395	51%
Austria	246	73	30%	0,13%	71	19	27%	51	29	57%	5	-	0%
Azerbaijan	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Belgium	1 804	1 316	73%	0,95%	427	299	70%	914	754	82%	5	-	0%
Bosnia and Herzegovina	13	8	62%	0,01%	1	-	0%	1	-	0%	-	-	0%
Bulgaria	5	3	60%	0,00%	1	-	0%	-	-	0%	-	-	0%
Canada	850	477	56%	0,45%	71	29	40%	129	104	81%	25	11	44%
Croatia	45	34	76%	0,02%	3	-	0%	2	2	100%	-	-	0%
Cyprus	38	21	55%	0,02%	-	-	0%	5	-	0%	-	-	0%
Czech Republic	333	204	61%	0,18%	216	115	53%	83	74	89%	-	-	0%
Denmark	362	225	62%	0,19%	119	62	52%	178	142	80%	5	-	0%
Dominican Republic	54	30	56%	0,03%	2	-	0%	19	18	95%	-	-	0%
Estonia	35	19	54%	0,02%	8	3	38%	14	9	64%	-	-	0%
Finland	144	102	71%	0,08%	35	29	83%	62	48	77%	1	-	0%
France	21 772	12 863	59%	11,49%	6 075	3 523	58%	8 766	7 007	80%	2 377	721	30%
Georgia	1	-	0%	0,00%	-	-	0%	-	-	0%	-	-	0%
Germany	25 519	13 801	54%	13,46%	6 452	3 252	38%	9 375	7 397	79%	4 786	1 467	31%
Hungary	345	159	46%	0,18%	38	-	0%	115	96	83%	7	-	0%
Iceland	3	2	67%	0,00%	-	-	0%	1	1	100%	-	-	0%
Italy	9 365	4 620	49%	4,94%	2 022	888	44%	1 769	1 242	70%	1 879	687	37%
Japan	1 617	1 010	62%	0,85%	252	199	79%	737	586	80%	-	-	0%
Latvia	2	2	100%	0,00%	-	-	0%	2	2	100%	-	-	0%
Lichtenstein	5	1	20%	0,00%	2	-	0%	-	-	0%	-	-	0%

2014	All providers			Requests share/all parties	Google and You Tube			Microsoft and Skype			Yahoo		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Lithuania	49	28	57%	0,03%	12	9	75%	15	10	67%	1	-	0%
Luxembourg	153	117	76%	0,08%	1	-	0%	138	111	80%	-	-	0%
Malta	377	197	52%	0,20%	99	57	58%	90	71	79%	9	-	0%
Mauritius	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Moldova	13	7	54%	0,01%	1	-	0%	5	3	60%	-	-	0%
Montenegro	7	1	14%	0,00%	-	-	0%	1	-	0%	-	-	0%
Netherlands	1 099	856	78%	0,58%	212	172	81%	734	607	83%	16	-	0%
Norway	363	238	66%	0,19%	93	48	52%	203	167	82%	12	-	0%
Panama	88	68	77%	0,05%	-	-	0%	88	68	77%	-	-	0%
Poland	1 747	550	31%	0,92%	1 046	307	29%	103	72	70%	1	-	0%
Portugal	2 223	1 356	61%	1,17%	647	346	53%	897	760	85%	18	-	0%
Romania	80	40	50%	0,04%	49	26	53%	-	-	0%	1	-	0%
Serbia	16	9	56%	0,01%	1	-	0%	-	-	0%	-	-	0%
Slovakia	107	36	34%	0,06%	62	5	8%	37	30	81%	3	-	0%
Slovenia	11	6	55%	0,01%	5	3	60%	2	2	100%	1	-	0%
Spain	4 462	2 391	54%	2,35%	1 394	690	50%	1 484	1 192	80%	429	114	27%
Sri Lanka	1	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Switzerland	462	266	58%	0,24%	254	169	66%	110	81	74%	12	-	0%
The former Yugoslav Republic of Macedonia	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Turkey	8 405	5 625	67%	4,43%	568	-	0%	7 130	5 411	76%	-	-	0%
Ukraine	8	2	25%	0,00%	5	1	20%	2	1	50%	-	-	0%
United Kingdom	20 127	13 894	69%	10,62%	3 615	2 665	74%	8 608	6 602	77%	2 978	1 141	38%
USA	80 703	63 147	78%	42,58%	22 520	18 318	81%	12 364	8 062	65%	11 656	9 680	83%
Total excl. USA	**108 829**	**64 901**	**60%**		**25 573**	**13 930**	**54%**	**44 206**	**34 545**	**78%**	**13 342**	**4 536**	**34%**
Total incl. USA	**189 532**	**128 048**	**68%**	**100%**	**48 093**	**32 248**	**67%**	**56 570**	**42 607**	**75%**	**24 998**	**14 216**	**57%**

2014	All providers			Requests share/all parties	Facebook			Twitter			Apple		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Albania	24	7	29%	0,01%	20	7	35%	1	-	0%	-	-	0%
Armenia	11	2	18%	0,01%	5	1	20%	-	-	0%	-	-	0%
Australia	6 438	4 236	66%	3,40%	1 439	937	65%	12	7	58%	175,0	37,6	21%
Austria	246	73	30%	0,13%	109	16	15%	-	-	0%	10,0	9,0	90%
Azerbaijan	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Belgium	1 804	1 316	73%	0,95%	448	260	58%	1	-	0%	9,0	3,0	33%
Bosnia and Herzegovina	13	8	62%	0,01%	11	8	73%	-	-	0%	-	-	0%
Bulgaria	5	3	60%	0,00%	3	3	100%	-	-	0%	1,0	-	0%
Canada	850	477	56%	0,45%	542	303	56%	62	18	29%	21,0	13,0	62%
Croatia	45	34	76%	0,02%	40	32	80%	-	-	0%	-	-	0%
Cyprus	38	21	55%	0,02%	33	21	64%	-	-	0%	-	-	0%
Czech Republic	333	204	61%	0,18%	33	15	45%	-	-	0%	1,0	-	0%
Denmark	362	225	62%	0,19%	46	17	37%	4	1	25%	10,0	3,0	30%
Dominican Republic	54	30	56%	0,03%	33	12	36%	-	-	0%	-	-	0%
Estonia	35	19	54%	0,02%	13	7	54%	-	-	0%	-	-	0%
Finland	144	102	71%	0,08%	46	25	54%	-	-	0%	-	-	0%
France	21 772	12 863	59%	11,49%	4 343	1 568	36%	96	11	11%	115,0	33,0	29%
Georgia	1	-	0%	0,00%	1	-	0%	-	-	0%	-	-	0%
Germany	25 519	13 801	54%	13,46%	4 669	1 592	34%	31	5	16%	206,0	87,7	43%
Hungary	345	159	46%	0,18%	185	63	34%	-	-	0%	-	-	0%
Iceland	3	2	67%	0,00%	2	1	50%	-	-	0%	-	-	0%
Italy	9 365	4 620	49%	4,94%	3 643	1 784	49%	10	2	20%	42,0	17,0	41%
Japan	1 617	1 010	62%	0,85%	11	1	9%	480	173	36%	137,0	51,0	37%
Latvia	2	2	100%	0,00%	-	-		-	-	0%	-	-	0%
Lichtenstein	5	1	20%	0,00%	3	1	33%	-	-		-	-	
Lithuania	49	28	57%	0,03%	20	9	45%	1	-	0%	-	-	0%
Luxembourg	153	117	76%	0,08%	5	2	40%	-	-	0%	9,0	4,0	44%

2014	All providers			Requests share/all parties	Facebook			Twitter			Apple		
Parties	Received	Disclosure	%		Received	Disclosure	%	Received	Disclosure	%	Received	Disclosure	%
Malta	377	197	52%	0,20%	178	68	38%	-	-	0%	1,0	1,0	100%
Mauritius	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Moldova	13	7	54%	0,01%	7	4	57%	-	-	0%	-	-	0%
Montenegro	7	1	14%	0,00%	6	1	17%	-	-	0%	-	-	0%
Netherlands	1 099	856	78%	0,58%	117	72	62%	9	2	22%	11,0	3,0	27%
Norway	363	238	66%	0,19%	46	20	43%	2	1	50%	7,0	2,0	29%
Panama	88	68	77%	0,05%	-	-		-	-	0%	-	-	0%
Poland	1 747	550	31%	0,92%	593	169	28%	-	-	0%	4,0	2,0	50%
Portugal	2 223	1 356	61%	1,17%	659	249	38%	1	-	0%	1,0	1,0	100%
Romania	80	40	50%	0,04%	30	14	47%	-	-	0%	-	-	0%
Serbia	16	9	56%	0,01%	15	9	60%	-	-	0%	-	-	0%
Slovakia	107	36	34%	0,06%	5	1	20%	-	-	0%	-	-	0%
Slovenia	11	6	55%	0,01%	3	1	33%	-	-	0%	-	-	0%
Spain	4 462	2 391	54%	2,35%	1 014	373	37%	112	13	12%	29,0	7,9	27%
Sri Lanka	1	-		0,00%	-	-	0%	1	-	0%	-	-	0%
Switzerland	462	266	58%	0,24%	71	12	17%	6	-	0%	9,0	4,0	44%
The former Yugoslav Republic of Macedonia	-	-		0,00%	-	-	0%	-	-	0%	-	-	0%
Turkey	8 405	5 625	67%	4,43%	318	210	66%	380	-	0%	9,0	4,0	44%
Ukraine	8	2	25%	0,00%	1	-	0%	-	-	0%	-	-	0%
United Kingdom	20 127	13 894	69%	10,62%	4 476	3 290	73%	144	52	36%	306,0	144,3	47%
USA	80 703	63 147	78%	42,58%	29 707	23 646	80%	2 879	2 203	77%	1 577,0	1 237,9	78%
Total excluding USA	**108 829**	**64 901**	**60%**		**23 242**	**11 178**	**48%**	**1 353**	**285**	**21%**	**1 113,0**	**427,5**	**38%**
Total including USA	**189 532**	**128 048**	**68%**	**100%**	**52 949**	**34 824**	**66%**	**4 232**	**2 488**	**59%**	**2 690,0**	**1 665,4**	**62%**

5.2 Policies and transparency reports of service providers: sources

5.2.1 Apple

http://www.apple.com/legal/privacy/en-ww/
http://images.apple.com/privacy/docs/legal-process-guidelines-emeia.pdf
http://www.apple.com/privacy/transparency-reports/

5.2.2 Google

https://www.google.com/transparencyreport/
https://www.google.com/transparencyreport/removals/government/?hl=en
https://www.google.com/transparencyreport/userdatarequests/?hl=en

5.2.3 Facebook

https://govtrequests.facebook.com/

5.2.4 Microsoft

https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/
https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr/
https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/crrr/

5.2.5 Twitter

https://support.twitter.com/articles/41949#
https://transparency.twitter.com/

5.2.6 Yahoo

https://transparency.yahoo.com/
https://transparency.yahoo.com/law-enforcement-guidelines/us

5.2.7 Other references and links[63]

Adobe
Law enforcement guide:
https://www.adobe.com/legal/compliance/law-enforcement.html
Transparency report:
https://www.adobe.com/legal/compliance/transparency.html

Amazon
Law enforcement guide:
http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf
Transparency report:
http://d0.awsstatic.com/certifications/Transparency_Report.pdf
Privacy notice:
http://www.amazon.com/gp/help/customer/display.html?nodeId=468496
Conditions of use:
https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088
Privacy and data security blog post:
http://blogs.aws.amazon.com/security/post/Tx35449P4T7DJIA/Privacy-and-Data-Security

[63] Established by the Electronic Frontier Foundation: Who has your back? Protecting your data from government requests https://www.eff.org/who-has-your-back-government-data-requests-2015

Apple
Law enforcement guide:
https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf
Transparency report:
https://www.apple.com/privacy/transparency-reports/
Government information requests:
https://www.apple.com/privacy/government-information-requests

AT&T
Law enforcement guide:
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/location-demands.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/emergency-requests.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/international.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html
Transparency report:
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html#sthash.BMut0WAH.dpuf

Comcast
Law enforcement guide:
http://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx
Transparency report:
http://corporate.comcast.com/images/Third-Comcast-Transparency-Report-2H2014-FINAL-02022015.pdf
Privacy notice:
http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html?CCT=53BA3D76CB1473BFF49C79FE4AA86DFF1EE2DE626F409A592CC8FD4F97F987FDED44763A4B54572047B30DDBC6AEBC5DCED6A73183C574B8E5697D9E3FD17293EB4FE71DF37B56C34FF77B9D0E092477A8C3958E8CC866906A7E34373B5718A30AEEF8F52C31E24CFFD314BC83C96E756A5AA0BA63C22EB0#When%20is%20Comcast%20required%20to%20disclose%20personally%20identifiable%20information%20and%20CPNI%20by%20law?
Statement on Upgrading the Security and Privacy of Your Email:
http://corporate.comcast.com/comcast-voices/upgrading-the-security-and-privacy-of-your-email

CREDO Mobile
Law enforcement guide:
http://www.credomobile.com/law-enforcement-guidelines
Transparency report:
http://www.credomobile.com/transparency

Privacy and security policy:
http://www.credomobile.com/privacy

Dropbox Transparency report:
https://www.dropbox.com/transparency
Government Data Request Principles:
https://www.dropbox.com/transparency/principles

Facebook
Law enforcement guidelines:
https://www.facebook.com/safety/groups/law/guidelines/
Transparency report:
https://govtrequests.facebook.com/
Data policy:
https://www.facebook.com/full_data_use_policy

Google
Legal process:
https://www.google.com/transparencyreport/userdatarequests/legalprocess/
Transparency report:
https://www.google.com/transparencyreport/
Dashboard data:
https://support.google.com/accounts/answer/162743?hl=en
Government requests to remove content:
https://www.google.com/transparencyreport/removals/government/

LinkedIn
Law enforcement guidelines:
https://help.linkedin.com/app/answers/detail/a_id/16880/~/linkedin-law-enforcement-data-request-guidelines
Transparency report:
https://www.linkedin.com/legal/transparency
Data request guidelines:
https://help.linkedin.com/ci/fattach/get/4773861/1431363803/redirect/1/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf

Microsoft
Principles, policies, and practices FAQ (law enforcement guidelines and other information):
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/
Transparency report
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
U.S. National Security Order Requests:
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/fisa/
Privacy statement:
http://www.microsoft.com/privacystatement/en-us/core/default.aspx#EHC
When transparency alone isn't enough:
http://blogs.microsoft.com/on-the-issues/2015/03/27/when-transparency-alone-isnt-enough/

Pinterest
Law enforcement guidelines:

https://help.pinterest.com/en/articles/law-enforcement-guidelines
Transparency report:
https://help.pinterest.com/en/articles/transparency-report-archive
Terms of service:
https://about.pinterest.com/en/terms-service

reddit
Transparency report (including law enforcement guidelines)
https://www.reddit.com/wiki/transparency/2014
What information we collect:
https://www.reddit.com/help/privacypolicy#section_what_information_we_collect

Slack
User data request policy:
https://slack.com/user-data-request-policy
Transparency report:
https://slack.com/transparency-report
Slack and transparency:
http://slackhq.com/post/117871977170/transparency
FAQ about privacy policy:
https://slack.zendesk.com/hc/en-us/articles/203950296-FAQs-about-Slack-s-Privacy-Policy
Privacy policy:
https://slack.com/privacy-policy

Snapchat
Law enforcement guidelines:
https://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604
Transparency report:
http://blog.snapchat.com/post/115310648870/our-transparency-report

Sonic
Law enforcement guidelines:
https://wiki.sonic.net/images/0/05/Sonic.net_Legal_Process_Policy.pdf
Transparency report:
https://corp.sonic.net/ceo/2014/04/28/2013-transparency-report/

Tumblr
Law enforcement guidelines:
https://www.tumblr.com/docs/en/law_enforcement
Transparency report:
https://www.tumblr.com/transparency

Twitter
Law enforcement guidelines:
https://support.twitter.com/articles/41949-guidelines-for-law-enforcement
Transparency report:
https://transparency.twitter.com/
Privacy policy
https://twitter.com/privacy?lang=en

Verizon
Transparency report and law enforcement guide:
http://transparency.verizon.com/us-report?/us-data
http://transparency.verizon.com/international-report

Wickr
Law enforcement guide
https://wickr.com/wp-content/uploads/2014/06/Law-Enforcement-Guidelines_5.12.14.pdf
Transparency report:
https://wickr.com/category/transparency-report/
Privacy policy:
https://wickr.com/privacy-policy/

Wikimedia
Law enforcement guide:
https://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines#What_We_Require_From_You
Transparency report:
https://transparency.wikimedia.org
https://transparency.wikimedia.org/content.html
Data retention guidelines:
https://meta.wikimedia.org/wiki/Data_retention_guidelines

Wordpress.com
Law enforcement guide:
https://en.support.wordpress.com/disputes/legal-guidelines/
Transparency report:
http://transparency.automattic.com/
Takedown demands:
http://transparency.automattic.com/takedown-demands/

Yahoo
Transparency report:
https://transparency.yahoo.com/
Law enforcement guide:
https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm
Content removals:
https://transparency.yahoo.com/government-removal-requests/index.htm
Users first statement:
https://transparency.yahoo.com/users-first/index.htm