Obtaining Electronic Evidence from the United States

OFFICE OF INTERNATIONAL AFFAIRS
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

3-4 November 2016

FOR LAW ENFORCEMENT USE ONLY
1. How should you preserve data?
2. What types of “electronic evidence” can we obtain for investigations?
3. Can you obtain the information directly from the communications service provider (CSP)? Or MLAT?
4. Legal Basis for request?
5. U.S. legal requirements for obtaining the types of electronic evidence that do require an MLAT?
Legal Basis for a Request

- Bilateral MLATs
- Budapest convention—parties include CA, CR, DR, PN, US; more than 40 in Europe
- UNTOC—covers most requests fraud, theft
- Inter-American/OAS Convention on MLA
- UNCAC, Narcotics or Terrorism Conv/ some cases
- Domestic Law of Requested State
The Need to Freeze
Preserve, Preserve, Preserve!

- CSPs in the United States are not required to maintain data for any specific period of time.
- Upon a request from the government, ECPA requires preservation of data for a period of 180 days (90 days, plus a 90-day extension).
- The major U.S. providers generally will voluntarily preserve data for longer periods of time if they know a foreign authority is pursuing the data through the MLAT process.
How to Preserve Data from Major CSPs?

- The major CSPs voluntarily accept requests from foreign authorities, so do not waste precious time submitting an MLAT request for preservation.
- As a general rule, they do not notify the subscriber of the preservation request.
- Check the CSP’s law enforcement guidelines for process.
- Record the tracking number; you will need to include it when making an MLAT request.
- Seek *timely* extensions until you receive the data.
If CSP says, “Not in US”

- Ask where the data is located
- Where will CSP accept service
- Later we’ll discuss Microsoft case
Categories of Electronic Evidence

- **Content**

- **Non-Content: transactional data**

- **Non-Content: subscriber data & access logs**

FOR LAW ENFORCEMENT USE ONLY
Non-Content: Subscriber Data

Name, address & phone number; email address used to register; means of payment (credit card, etc.)
Non-Content: Access Logs

Dates, times and IP addresses for each log-in
No MLAT Required!

Fortunately, to obtain *subscriber information and access logs*, the major CSPs generally accept requests directly from LE authorities, without requiring a request from the U.S. government.

CSPs provide this information on a *voluntary basis* and are not required to do so.

Check the law enforcement guide of the relevant CSP for its specific policies.
Should You Ask the CSP Directly?

**Advantage**: Avoid the time-consuming MLAT process and receive your evidence much more quickly.

**Possible Disadvantage**: Notifying the subscriber.
- Some CSPs will notify the subscriber in the absence of a U.S. court order prohibiting notification.
- You need to determine the CSP’s notification policy.
- If there is no problem with the subscriber being notified, you should seek the data directly from the CSP if you are able. Otherwise, you need to do an MLAT request specifying that the subscriber should not be notified.
Subscriber Data & Access Logs: Legal Standard

- Electronic Communications Privacy Act (ECPA);
- **Standard**: Relevant and related to the criminal investigation
- Provide information regarding why notification to the subscriber would harm the investigation
- Executing U.S. authority can obtain a protection order from the court, prohibiting notification to the subscriber (18 U.S.C. § 2705(b))
Non-Content: Transactional Data

Sender and recipient, including their IP addresses;
Dates and times of communications;
Duration or “size” of communications
Email Non-Content Data: Everything EXCEPT Subject and Messages

<table>
<thead>
<tr>
<th>Date: Today</th>
<th>Subject</th>
<th>Received</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiona Alexander</td>
<td></td>
<td>Thu 2/4/2010 1:44 PM</td>
<td>46 KB</td>
</tr>
<tr>
<td>Libin, Nancy C. (</td>
<td></td>
<td>Thu 2/4/2010 1:38 PM</td>
<td>40 KB</td>
</tr>
<tr>
<td>Springsteen, Joseph</td>
<td></td>
<td>Thu 2/4/2010 1:37 PM</td>
<td>22 KB</td>
</tr>
<tr>
<td>Springsteen, Joseph</td>
<td></td>
<td>Thu 2/4/2010 1:34 PM</td>
<td>27 KB</td>
</tr>
<tr>
<td>Caputo, Renee</td>
<td></td>
<td>Thu 2/4/2010 1:22 PM</td>
<td>116 KB</td>
</tr>
<tr>
<td>Gull, Jason</td>
<td></td>
<td>Thu 2/4/2010 12:50 PM</td>
<td>20 KB</td>
</tr>
<tr>
<td>Shave, Betty</td>
<td></td>
<td>Thu 2/4/2010 12:34 PM</td>
<td>141 KB</td>
</tr>
<tr>
<td>Shave, Betty</td>
<td></td>
<td>Thu 2/4/2010 12:19 PM</td>
<td>17 KB</td>
</tr>
<tr>
<td>Williams, Evan</td>
<td></td>
<td>Thu 2/4/2010 12:07 PM</td>
<td>15 KB</td>
</tr>
<tr>
<td>Lerner, Jay</td>
<td></td>
<td>Thu 2/4/2010 11:56 AM</td>
<td>25 KB</td>
</tr>
<tr>
<td>Rusch, Jonathan</td>
<td></td>
<td>Thu 2/4/2010 11:53 AM</td>
<td>31 KB</td>
</tr>
<tr>
<td>Downing, Richard</td>
<td></td>
<td>Thu 2/4/2010 11:49 AM</td>
<td>30 KB</td>
</tr>
<tr>
<td>Corn, Gavin</td>
<td></td>
<td>Thu 2/4/2010 11:19 AM</td>
<td>4 KB</td>
</tr>
<tr>
<td>Cox, Howard</td>
<td></td>
<td>Thu 2/4/2010 11:19 AM</td>
<td>4 KB</td>
</tr>
<tr>
<td>Dougherty, Thomas</td>
<td></td>
<td>Thu 2/4/2010 11:19 AM</td>
<td>4 KB</td>
</tr>
<tr>
<td>Weiss, Corbin</td>
<td></td>
<td>Thu 2/4/2010 11:19 AM</td>
<td>4 KB</td>
</tr>
</tbody>
</table>
AKA “Header Information”

Sun, 25 Oct 2014 04:07:56 -0700 (PDT)
From: Giovanni Smith <giovannismith@gmail.com>
Content-Type: multipart/alternative;
boundary="Apple-Mail-635C56A5-9628-4A4B-867F-0B4CCBAB1D40"
To: "Posa, Cristina" <cristina@eurojustconference.com>
X-Mailer: iPhone Mail (11D257)
Transactional Data: Legal Standard

Burden of proof to obtain a “2703(d) order”:

- **Specific and articulable facts** showing reasonable grounds to believe that records are **relevant and material** to ongoing law enforcement investigation

Sealing and protection orders

- we have to provide justification to the court
Example of “Specific and Articulable Facts”

The police arrest a subject in a child pornography case and seize his smartphone.

They search his Gmail app and see that he is in contact with others using obviously fake identities to receive and distribute child pornography.

You already have the contents of the messages, but you need **the IP addresses of the recipients** so that you can begin to locate and identify them.

Make an MLAT request for this IP information for the relevant time period.
Sealing and Protection Orders

Must provide justification to the court

Reason to believe that notification will result in:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence;
- intimidation of potential witnesses; or
- otherwise seriously jeopardizing an investigation or unduly delaying a trial
Obtaining Content

FOR LAW ENFORCEMENT USE ONLY
Amendment IV
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
Search Warrant

1. U.S. judge must issue a search warrant
2. Based on a sworn affidavit of a U.S. agent
3. Demonstrating probable cause that
4. The account will contain the evidence, fruits or instrumentalities of a crime.
What does “Probable Cause” Mean in this Context?

- Probable cause that the account will contain evidence of the crime.
- It is not enough to state that the person committed the crime – you must link it to the account to be searched.
What does “Probable Cause” Mean in this Context?

Conclusions are not sufficient.

You must precisely describe facts gathered by the investigators demonstrating that it is probable that the account contains evidence of a crime.

The description of facts must provide the sources of the facts, and enough information about them to enable the U.S. judge to assess their reliability.

The facts must be recent enough that the judge can conclude that it is probable that the evidence is still in the account.
“Building” Probable Cause

- Preservation
- Subscriber info and access logs
- Transactional Data (senders and recipients)
- Content

FOR LAW ENFORCEMENT USE ONLY
Compelled Production: Changes Following the *Microsoft* Decision

July 2016: The U.S. Court of Appeals for the Second Circuit issued a decision narrowing the ability to compel data from CSPs to data located in the United States.

Major CSPs are applying the ruling nationwide and limiting the production of content.

Preservation and the production of non-content data also may be limited.

If data sought is outside the United States, a request to us may be fruitless; you may be able to obtain it from another country.

New requirement prior to submitting MLAT request:
- Identify the location(s) of the data associated with the account, and
- Identify the country or countries where the CSP will accept service of process ordering production of that data.
Some Notes on Obtaining Evidence via MLAT

In 2009, U.S. law changed and 18 U.S.C. § 3512 was enacted, allowing for more rapid execution of foreign requests.

If you are aware of a related U.S. federal investigation or prosecution, please mention this in the request.

OIA has devoted additional resources to the review and execution of foreign requests for provider data and to develop and provide expertise in this area.
Drafting Tips for the Request

- Be mindful when requesting urgency.
- Make sure to provide factual information regarding the use of each separate account for which records are sought.
- Provide a relevant date range for requested records.
- Make sure that the account name is spelled correctly and consistently throughout the request.
- There is no need to attach all full witness statements to the request.
Police-to-Police Sharing

If your investigators have contacts with U.S. investigators, such as the FBI, DEA, ICE, or U.S. Secret Service Legal Attaché at the embassy, ask them if the United States already has an open investigation.

If so, the U.S. agency may be able to share evidence on a police-to-police basis, perhaps with certain limitations and restrictions on use.
Emergency Disclosures
Emergency Disclosures

- We can help you make a request for emergency voluntary disclosure when there is no time for an MLAT request (18 U.S.C. § 2702).
- Applies only to terrorism or non-terrorism cases involving imminent danger of death or serious injury, such as kidnapping cases.
- Contact the FBI, in particular the Legal Attaché for your country.
- CCIPS (the US’s 24/7 Network point of contact) or OIA can also help, but first try the FBI.
Need More Information?

- Further detailed info is provided in:
  - Brief Guide to Obtaining Mutual Legal Assistance and Extradition from the United States, and
  - Investigative Guide for Obtaining Electronic Evidence from the United States

- We are here to help!
Questions?

Magdalena Boynton
Magdalena.Boynton@usdoj.gov

Thomas Burrows
Thomas.Burrows@usdoj.gov