EU/COE Joint Project on Global Action on Cybercrime

Legislation on cybercrime: Substantive criminal law

Joint ECOWAS-Council of Europe regional conference

Mutual Assistance Requests: Procedures for requesting electronic evidence from international partners

Abuja, Nigeria – 11 September 2017

Zahid Jamil
Council of Europe Expert, Pakistan
The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and related standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

“Protecting you and your rights in cyberspace”
Budapest Convention on Cybercrime
**Budapest Convention: scope**

**Criminalising conduct**
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

**Procedural tools**
- Expedited preservation
- Partial disclosure of traffic data
- Production orders
- Search and seizure
- Interception of computer data

**International cooperation**
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

**Harmonisation**
International Cooperation
Informal Cooperation

- Discretionary
- Faster when works
- Seldom work
- Not evidence
- Usually uneven playing field
- Usually refusals
Examples:
Formal Cooperation: Treaty or Convention

- Bilateral MLATs
- Archaic provisions
- Slow
- Not always lead to cooperation
- Every country
- Not a cyber solution
- Need modernization
- One country at a time
- Regional - geographic limitations
Examples:
NEED:

Formal International obligation
Catches up with the speed of informal process
Human rights
Confidence & Trust
Limited to criminal justice
• Harmonize laws
• Not technologically specific or else become archaic
• Not have everything or else no consensus.
• Baseline. Inclusive treaty.
• Harmonize procedures
• Harmonized cross border procedures and cooperation
• Not mutually exclusive. Complimentary
• Members include those where data held and cooperation sought
Majority of Request Flows:

Infrastructure States to Developing States
Case Study: Avalanche Network
Consider this situation:

- **600 servers globally**
- **1,000,000 emails per day with malware**
- **800,000 Domains used**
- **Victims in 180 countries**
- **500,000 infected devices**
Consider this situation:

**BOTNET**

**Phishing**

**17 different Malware types**

**Banking Trojans**

**DDoS Attacks**

**Moneymule schemes**

**Malware campaigns**
Could you cope?

**Avalanche Crime Network**
- Started with a Ransomware attack in Germany
- Four year investigation by German Police
- 30 November 2016 swoop
- 30 countries involved with FBI, Europol, Interpol
- 37 premises searched
- 39 servers seized, 221 servers put off-line

How many arrests? 20? 50? 100?

**Just 5 arrests**
30 countries - Prosecutors & Investigators
5 arrested
37 premises searched
39 servers seized
Over 180 countries Victims of malware identified
221 servers offline
(abuse notifications to hosting providers)

Over 800,000 domains seized, sinkholed or blocked
Largest-ever use of sinkholing to combat botnet infrastructures unprecedented in scale

FIGURES AT A GLANCE
Countries involved: Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.

Arrests: 5
Searches conducted: 37
Servers seized: 39
Servers taken offline through abuse notifications: 221
Operation Avalanche

1st layer
Double Fast Flux

Potentially millions of infected devices connected to the internet request to connect to a list of addresses.

Computers connected to the internet use name servers to resolve human readable domain names into the IP addresses used to route the IP network traffic (e.g., www.europol.europa.eu has the following IP: 158.169.131.22). Usually one domain is delegated to one IP address for a long period of time.

A Domain Generation Algorithm (DGA) generates thousands of new domain names every day. hellosd4f.com, hellog7hr.com, helloyz1.com, ....

A request to connect is made to the domain.

Name Server
is used to resolve the domain name

Fast Flux: the name server record changes every five minutes (300s) - TTL (time to live)

The technique known as Fast Flux involves automatically and frequently changing the IP address records associated with a domain name. Single Fast Flux changes the IP address used to host address records associated with a domain (such as a website name). Double Fast Flux changes both the IP address records and the name server that is used to resolve the domain too.

IP Address Record
provides the IP address of the domain

Fast Flux: the IP addresses change every five minutes (300s) - TTL (time to live)

2nd layer
Proxy layer

Network of compromised computers
multiple individual computers are used to host the domain for a short period of time.

redirect to a proxy
Name Server

is used to resolve the domain name

Fast Flux: the name server record changes every five minutes (300s) - TTL (time to live)

domain and the name servers that resolve it, with the aim of making it more difficult for Law Enforcement to trace and take down hosted criminal infrastructures.

IP Address Record

provides the IP address of the domain

Fast Flux: the IP addresses change every five minutes (300s) - TTL (time to live)

Network of compromised computers

multiple individual computers are used to host the domain for a short period of time

redirect to a proxy

The proxies redirect the traffic and are used to disguise the originating source of these instructions.

Cluster infrastructure

The criminals controlling the clusters are anonymous.

Will normally point to an IP where bots go for registration, to receive instructions, or to activate attacks.

redirects to the criminal cluster infrastructure and splits per botnet
Cluster infrastructure

The criminals controlling the cluster can now give instructions to and/or extract data from your computer.

- Money muling
- Malware
  - Gozy malware
  - URLzone malware
  - Rovnix malware
  - TeslaCrypt malware

3rd layer

Backend infrastructure

Administration infrastructure

redirects to the criminal cluster infrastructure and splits per botnet
Sinkholing

is an action whereby *traffic* between infected computers and a criminal infrastructure is *redirected to servers controlled by law enforcement* authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses.

When employed at a **100% scale, infected computers can no longer reach the criminal command and control computer systems** and so criminals can **no longer control the infected computers**.

The sinkholing infrastructure captures victims’ IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.
Prosecutor's Office Paid Bitcoin Ransom in Cyberattack

By JOE MANDAK, ASSOCIATED PRESS -
PITTSBURGH — Dec 5, 2016, 6:56 PM ET

A state prosecutor's office in Pennsylvania was among hundreds of thousands of victims of a now-shuttered international cybercrime operation, paying nearly $1,400 in a bitcoin ransom to free up its infected computer network, authorities disclosed Monday.

Federal prosecutors said in court documents only that an unidentified state government entity had been victimized by the ring known as the Avalanche network. But the Allegheny County district attorney, Stephen Zappala Jr., confirmed to The Associated Press that it was his office.

The disabling of the Avalanche network by the European Union and U.S. authorities was announced last week in Europe. Federal documents unsealed in Pittsburgh on Monday provided additional details.

The Avalanche group had operated since at least 2010 and infected at least 500,000 computers worldwide, said Soo Song, acting U.S. Attorney in Pittsburgh.

"The takedown of Avalanche was unprecedented in its scope, scale, reach and level of cooperation among 40 countries," Song said.
Feds: Business lost $387,500 in world cybercrime operation

A Pennsylvania business lost more than $387,000 in an international cybercrime operation disabled by federal authorities and the European Union last week.

Federal prosecutors and FBI agents in Pittsburgh on Monday plan to offer more details from last week’s sweep of the Avalanche network. The group is accused of inflicting hundreds of millions of dollars in losses worldwide before it was dismantled and five key suspects were arrested.

Documents unsealed Monday show a business in Carnegie lost $387,500 when someone drained the money from the company’s online account.

Another business in New Castle was twice targeted with unsuccessful efforts to steal more than $120,000.

The U.S. Department of Justice has accused the network of hosting some of the world’s most pernicious malware as well as several money laundering campaigns.

Explore further: Police make 5 arrests in ‘unprecedented’ cybercrime takedown
What challenges involved in Avalanche Operation?
What challenges involved in Avalanche Operation?

Where were the servers?
Where were the perpetrators?
Who were the perpetrators?
Who to lead investigation?
Who & where were the victims?
What format is needed for required evidence?
How disable/delete the malware?
What evidence required?
Where is the required evidence?
What damage was done?
What malware used?
How identify investigative partners?
How to request required evidence?
Who & where to prosecute?
Operation Avalanche

**Issues breakdown into:**
- Legal
- Procedural
- Practical

**What about?**
- Political?
- Economic?
- Cultural?
Case Study: Axact – Global Diploma Mill
Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions

By DECLAN WALSH   MAY 17, 2015

Axact, which has its headquarters in Karachi, Pakistan, ostensibly operates as a software company.
Sara Fard for The New York Times

Seen from the Internet, it is a vast education empire: hundreds of universities and high schools, with elegant names and smiling professors at sun-dappled American campuses.

Their websites, glossy and assured, offer online degrees in dozens of disciplines, like nursing and civil engineering. There are glowing endorsements on the CNN iReport website, enthusiastic video testimonials, and State Department authentication certificates bearing the signature of Secretary of State John Kerry.

“We host one of the most renowned faculty in the world,” boasts a woman introduced in one promotional video as the head of a law school. “Come be a part of Newford University to soar the sky of excellence.”
Take down of a Global Organized Crime Syndicate

• Swift Action
• Over 700 TB of data
• Over 14,000 websites
• Legal entities all over the world
• Cross-border money trails
• Protecting US, UK, Australia, UAE, Saudi and other citizens and Governments
<table>
<thead>
<tr>
<th>Country Name</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>135</td>
</tr>
<tr>
<td>Aland Islands</td>
<td>1</td>
</tr>
<tr>
<td>Albania</td>
<td>28</td>
</tr>
<tr>
<td>Algeria</td>
<td>78</td>
</tr>
<tr>
<td>American Samoa</td>
<td>4</td>
</tr>
<tr>
<td>Andorra</td>
<td>1</td>
</tr>
<tr>
<td>Angola</td>
<td>152</td>
</tr>
<tr>
<td>Morocco</td>
<td>40</td>
</tr>
<tr>
<td>Mozambique</td>
<td>32</td>
</tr>
<tr>
<td>Myanmar</td>
<td>43</td>
</tr>
<tr>
<td>Namibia</td>
<td>19</td>
</tr>
<tr>
<td>Nauru</td>
<td>7</td>
</tr>
<tr>
<td>Nepal</td>
<td>29</td>
</tr>
<tr>
<td>Netherlands</td>
<td>241</td>
</tr>
<tr>
<td>Netherlands Antilles</td>
<td>7</td>
</tr>
<tr>
<td>New Zealand</td>
<td>73</td>
</tr>
<tr>
<td>Nicaragua</td>
<td>3</td>
</tr>
<tr>
<td>Niger</td>
<td>19</td>
</tr>
<tr>
<td>Nigeria</td>
<td>461</td>
</tr>
<tr>
<td>Student ID</td>
<td>University</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>EU-2006-12</td>
<td>Ashwood University</td>
</tr>
<tr>
<td>D-2006-12</td>
<td>Rochville University</td>
</tr>
<tr>
<td>D-2006-12</td>
<td>Rochville University</td>
</tr>
<tr>
<td>D-2006-12</td>
<td>Rochville University</td>
</tr>
<tr>
<td>D-2006-12</td>
<td>Rochville University</td>
</tr>
<tr>
<td>D-2006-12</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AD-2006-12 127351</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AU-2006-12 98165</td>
<td>Ashwood University</td>
</tr>
<tr>
<td>AD-2006-12 230061</td>
<td>Rochville University</td>
</tr>
<tr>
<td>ID</td>
<td>University</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>AD-2006-12 302654</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AD-2006-12 223685</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AD-2006-12 92898</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AD-2006-9-307831</td>
<td>Rochville University</td>
</tr>
<tr>
<td>BU-2006-8-392441</td>
<td>Belford University</td>
</tr>
<tr>
<td>Course Code</td>
<td>Institution</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>AMUO-2014-08-111439</td>
<td>Almeda University Online</td>
</tr>
<tr>
<td>AMUO-2014-09-111524</td>
<td>Almeda University Online</td>
</tr>
<tr>
<td>AD-2006-9-307831</td>
<td>Rochville University</td>
</tr>
<tr>
<td>AU-2006-12-53228</td>
<td>Ashwood University</td>
</tr>
<tr>
<td>AD-2006-12-229196</td>
<td>Rochville University</td>
</tr>
</tbody>
</table>
• Pakistan not a member of:
  ➢ Warsaw Convention
  ➢ Budapest Convention

• No mechanism for cross-border exchange of electronic evidence and financial trails

• Innovation was the only option to successfully cooperate internationally, pursue case and freeze assets
Spontaneous Information

• Request submitted to FBI for information resulted in so much information that the request in effect became spontaneous interagency information sharing

• Enabled FBI to initiate its investigation and ultimately send letter to FIA that was to be used as evidence in court
• Law enforcement agency cooperated directly with US Federal Trade Commission

• Cross border exchange – data had to be sent on physical storage devices (equivalent to over 10,000 pages of data)

• Received prompt response after FTC conducted its internal investigation based upon data provided to it
Cross-border Cooperation with Private Sector

• Exchange of data between FIA and Michigan private attorneys resulted in quicker freezing of assets abroad.

• No need to go to Pakistan MoFA and Embassy to US DoS, DoJ and FBI.

• Michigan attorneys provided corporate data available to them.
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

CARRIE MCCLUSKEY, et al.,
Plaintiffs,

v.

BELFORD HIGH SCHOOL, et al.,
Defendants.

Case No. 4:09-cv-14345-MAG-MKM
Hon. Mark A. Goldsmith

DECLARATION OF SHOAIB SHAIKH

Shoaib Shaikh, declares as follows:

1. I am more than 18 years of age and am competent to make this declaration.

2. I am a director of Garnishee Defendants Tullow, Inc. and Tinko, Inc. ("Garnishee Defendants").

3. I make this Declaration based on personal knowledge.

4. Garnishee Defendants are Delaware companies that provide global online payment processing services as resellers/billing providers for online businesses (similar to 2checkout.com).
5. Garnishee Defendants have no employees, offices or property in the State of Michigan.

6. I am responsible for the Garnishee Defendants’ operations, which are automated services. When I needed to perform work for the Garnishee Defendants, I did that work from my home or office in Pakistan. Any technical work was outsourced to Axact FZ LLC in United Arab Emirates when needed.

7. Currently, and for approximately the past nine months, I have been detained by Pakistani law enforcement authorities and am in their custody.

8. As a result of being detained by Pakistani law enforcement authorities, I am not permitted to travel to the United States for any depositions noticed by Plaintiffs in the above captioned matter. I also would not be able to obtain a Visa to travel to the United States.

9. I am the most knowledgeable person to testify as a corporate representative on behalf of Garnishee Defendants regarding the operations of Garnishee Defendants and the topics identified in any depositions noticed by Plaintiffs of Garnishee Defendants in the above captioned matter.

10. Even if I could travel, it would be unduly burdensome and costly to travel to Michigan for the noticed depositions.
FIR No. 7 of 2015 - dated 27.05.2015
(State vs. M/s. Axact (Pvt) Ltd.) - FIA, Corporate Crime Circle, Karachi

With reference to the above noted matter, the ongoing investigation has revealed substantial crucial evidence that is outside Pakistan which requires Request for Legal Assistance from the US Department of Justice in general and the Office of International Judicial Assistance, in particular and Federal Bureau of Investigation for the following:

1. Request that digital evidence which is at risk of destruction and removal (through erasure/deletion) and hence volatile requiring urgent action through cooperation on the part of the US Government and law enforcement be secured, preserved and transmitted as evidence to Pakistan to aid the investigation and prosecution of the above noted matter (details of service providers and the data to be preserved and other details enumerated in Annex A)

2. Assistance in recording statements of customers/victims (contact details listed at Annex B)

3. Request confirmation/corroboration of the inauthenticity of the degrees/accreditations/diplomas/certifications suspected to be or identified as fake, fraudulent and forged, that have been issued by the non-existent educational and other institutions through the use of “spoofed” inauthentic, fraudulent and forged websites (details enumerated in Annex C)

4. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic legalizations, attestations, notarizations, apostilles, seals and approvals attributed to the US Department of State, US Government and Notaries. (details enumerated in Annex D)

5. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic Schools and Universities. (details enumerated in Annex DD)

6. Request disclosure of the bank account statements for each bank account identified in Annex E from the time of its opening until 30th July 2015 or at least initially statements for the last 7 years

10. Request information and details of the shareholding and identity of the shareholders, directors, officers, company secretaries, any authorized signatories for or on behalf of legal entities identified in Annex F along with, if available, the nationality(s), address(es), any contact details or other details that may be available with respect to the aforesaid persons

11. Request that the prosecution be permitted to present the information and documents received before the competent courts in Pakistan in connection with the criminal proceedings and ancillary proceedings regarding the proceeds of crime and money laundering, unless otherwise specified

12. Request the provision of the transcripts, pleadings, orders, judgments and records of the proceedings before the United States District Court Eastern District Of Michigan Southern Division in Civil Action No. 09-CV-14345 ELIZABETH LAUBER, et al., vs. BELFORD HIGH SCHOOL, et al., (http://www.belfordlawsuit.com/)

13. Assistance between prosecutorial/investigative team leads and their counterparts on an ongoing basis with respect to this case

The undersigned requests that necessary urgent cooperation and assistance in this criminal matter may kindly be sought from the foreign Governments, law enforcement authorities as well as corporations/businesses to aid the investigation. This office is also willing and able to provide any assistance for the preparation of such requests given the complexity, volume and countries involved as may be deemed necessary by the competent authority.

Submitted for your kind consideration and urgent approval.
Memorandum

Office of the Director
FIA Islamabad Zone
Express Way-Iqbal Town
Islamabad, Pakistan

File No. IS-C163-A
NY-6434502

Office of the Legal Attaché
United States Embassy
Islamabad, Pakistan

8 February 2016

(U/REL TO USA, PAK) As your Service is aware, the FBI has been investigating a Pakistan-based entity named Axact. Ongoing investigation has identified a "diploma mill", orchestrated by Axact and headquartered in Karachi, Pakistan. Among engaging in other nefarious activity, Axact's primary scheme of illegality pertains to soliciting the sale of fictitious college and high school diplomas to both willing and unwilling purchasers. The vast majority of purchasers have been identified as located both within the United States and throughout the Middle East.

(U/REL TO USA, PAK) In furtherance of this scheme, Axact has established a worldwide web of shell companies and associates. The shell companies have been used to veil Axact funds and proceeds to further facilitate the transport of the fictitious diplomas, as well as to enhance the illusion that the diplomas were from legitimate educational institutions (e.g., via securing fictitious accreditation either within the United States or abroad).

(U/REL TO USA, PAK) Regarding financial accounts located in the United States, Axact appears to have set up three primary shell companies in the United States, by the names of Mivvel Inc., Tullow Inc., and Tinko Inc., as well as various tertiary shell companies, to include, but not limited to Blitace Inc. The Directors of said entities have been identified to include both Pakistani-based Axact executives, as well as United States-based individuals.

(U/REL TO USA, PAK) Vasg Asic, the Chief Operating Officer of Axact, holds 49% of the shares of Mivvel Inc. Shabir Ahmed, and the Owner/President of Axact, holds 49% of the shares of Tullow and Tinko. With respect to Mivvel Inc., the remaining 51% of the shares belong to Ali Gaffar Vajjora, date of birth 23 March 1971, 109 Juliett Fowler Street, # B-303, Dallas, Texas.

(U/REL TO USA, PAK) With respect to Tinko and Tullow, the majority share holders are Zubair Syed (Tullow), date of birth 27 October 1962, and Urma Shiehen (Tinko), date of birth 7
Being able to demonstrate:

• best practice procedures/processes were in place
• responsibilities were allocated
• assisted in information exchange and led to greater international cooperation, for instance, from:
  
  ➢ Michigan lawyers
  ➢ FBI
  ➢ FTC
International co-operation tools

- Operational and procedural rules
- Common to other international conventions
- Some of them, very innovative
Mutual Legal Assistance
Budapest Convention on Cybercrime

- Default
- Extradition
- Legal Mutual Assistance
- Spontaneous Information
- Confidentiality and limitation on use
- Expedited preservation of stored computer data
- Expedited disclosure of preserved traffic data
- Mutual assistance regarding
  - accessing of stored computer data
  - access to real-time collection of traffic data
  - interception of content data
- 24/7 Network
- Trans border Access
Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions

By DECLAN WALSH MAY 17, 2015

Axact, which has its headquarters in Karachi, Pakistan, ostensibly operates as a software company.
Sara Farid for The New York Times

Seen from the Internet, it is a vast education empire: hundreds of universities and high schools, with elegant names and smiling professors at sun-dappled American campuses.

Their websites, glossy and assured, offer online degrees in dozens of disciplines, like nursing and civil engineering. There are glowing endorsements on the CNN iReport website, enthusiastic video testimonials, and State Department authentication certificates bearing the signature of Secretary of State John Kerry.

“We host one of the most renowned faculty in the world,” boasts a woman introduced in one promotional video as the head of a law school. “Come be a part of Newford University to soar the sky of excellence.”
Spontaneous information disguised as MLA request

FIR No. 7 of 2015 - dated 27.05.2015
(State vs. M/s. Axact (Pvt) Ltd.) - FIA, Corporate Crime Circle, Karachi

With reference to the above noted matter, the ongoing investigation has revealed substantial crucial evidence that is outside Pakistan which requires Request for Legal Assistance from the US Department of Justice in general and the Office of International Judicial Assistance, in particular and Federal Bureau of Investigation for the following:

1. Request that digital evidence which is at risk of destruction and removal (through erasure/deletion) and hence volatile requiring urgent action through cooperation on the part of the US Government and law enforcement be secured, preserved and transmitted as evidence to Pakistan to aid the investigation and prosecution of the above noted matter (details of service providers and the data to be preserved and other details enumerated in Annex A)

2. Assistance in recording statements of customers/victims (contact details listed at Annex B)

3. Request confirmation/corroborate of the inauthenticity of the degrees/accreditations/diplomas/certifications suspected to be or identified as fake, fraudulent and forged, that have been issued by the non-existent educational and other institutions through the use of “spoofed” inauthentic, fraudulent and forged websites (details enumerated in Annex C)

4. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent and inauthentic legalizations, attestations, notarizations, apostilles, seals and approvals attributed to the US Department of State, US Government and Notaries. (details enumerated in Annex D)

5. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic Schools and Universities. (details enumerated in Annex DD)

6. Request disclosure of the bank account statements for each bank account identified in Annex E from the time of its opening until 30th July 2015 or at least initially statements for the last 7 years

10. Request information and details of the shareholding and identity of the shareholders, directors, officers, company secretaries, any authorized signatories for or on behalf of legal entities identified in Annex F along with, if available, the nationality(s), address(es), any contact details or other details that may be available with respect to the aforesaid persons

11. Request that the prosecution be permitted to present the information and documents received before the competent courts in Pakistan in connection with the criminal proceedings and ancillary proceedings regarding the proceeds of crime and money laundering, unless otherwise specified

12. Request the provision of the transcripts, pleadings, orders, judgments and records of the proceedings before the United States District Court Eastern District Of Michigan Southern Division in Civil Action No. 09-CV-14345 ELIZABETH LAUBER, et al., vs. BELFORD HIGH SCHOOL, et al., (http://www.belfordlawsuit.com/)

13. Assistance between prosecutorial/investigative team leads and their counterparts on an ongoing basis with respect to this case

The undersigned requests that necessary urgent cooperation and assistance in this criminal matter may kindly be sought from the foreign Governments, law enforcement authorities as well as corporations/businesses to aid the investigation. This office is also willing and able to provide any assistance for the preparation of such requests given the complexity, volume and countries involved as may be deemed necessary by the competent authority.

Submitted for your kind consideration and urgent approval.
Spontaneous information disguised as MLA request

File No. IS-C163-A
NY-6434502

Office of the Director
FIA Islamabad Zone
Express Way-Iqbal Town
Islamabad, Pakistan

8 February 2016

Office of the Legal Attaché
United States Embassy
Islamabad, Pakistan

As your Service is aware, the FBI has been investigating a Pakistan-based entity named Axact. Ongoing investigation has identified a "diploma mill," orchestrated by Axact, and headquartered in Karachi, Pakistan. Among engaging in other nefarious activity, Axact's primary scheme of illegality pertains to soliciting the sale of fictitious college and high school diplomas to both willing and unwitting purchasers. The vast majority of purchasers have been identified as located both within the United States and throughout the Middle East.

In furtherance of this scheme, Axact has established a worldwide web of shell companies and associates. The shell companies have been used to veil Axact funds and proceeds; to further facilitate the transport of the fictitious diplomas, as well as to enhance the illusion that the diplomas were from legitimate educational institutions (e.g. via securing fictitious accreditation either within the United States or abroad).

Regarding financial accounts located in the United States, Axact appears to have set up three primary shell companies in the United States, by the names of Mivvel Inc., Tullow Inc., and Tinko Inc., as well as various tertiary shell companies, to include, but not limited to Blitzace Inc. The Directors of said entities have been identified to include both Pakistani-based Axact executives, as well as United States-based individuals.

Vigas Attia, the Chief Operating Officer of Axact, holds 49% of the shares of Mivvel Inc. Shoab Ahmed, and the Owner/President of Axact, holds 49% of the shares...
Article 26
Spontaneous Information

1 - A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
Article 26
Spontaneous Information

2 - Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.
Spontaneous Information

- The authorities from a Party, within an internal investigation, discover that some of the information they obtained must be forwarded to the authorities of other Party.
- It can be done if the information seems to be useful or necessary to the beginning or the developing of an investigation respecting to a criminal offence in the framework of the Convention.
- According to Article 26, 2, this dispatch of information can be submitted to certain conditions, mainly of confidentiality.
1 - A Party may request another Party to **order or otherwise obtain** the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
Article 29

- **Expedited preservation** of data stored in a computer system
- Parallel framework to the internal provision
  - allows one contracting Party to require from other Party the expedited preservation of data
  - if at the same time expresses its intention of sending a formal request of assistance for a search, or a seizure, or any similar measure
- The requested party must act with due diligence, to preserve requested data, according to its own national law
- Dual criminality cannot be required by the requested party, as condition for preservation of data (except offenses other than Art 2-11 or political, sovereignty, security, public order, or other essential interests)
Requesting Expeditious Preservation

• Specify:
  • Authority seeking preservation
  • Offence that is subject of criminal investigation
  • Brief summary of facts of case
  • Stored computer data to be preserved
  • Any available information on custodian of data or location of computer system
  • Necessity of preservation
  • That party intends to submit request for MLA
**Requesting Expeditious Preservation**

- **Grounds for refusals:**
  - **Dual criminality only if** party requires dual criminality as condition for responding to other mutual legal assistance requests and believes that condition will not be met (*i.e.* offenses other than Art 2-11)
  - Request in relation to **political offence**
  - Execution of request will **prejudice sovereignty, security, ordre public** or other essential interests

- **Period of preservation** – **at least 60 days**
Article 30
Expedited Disclosure of Preserved Traffic Data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.
Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via Belarus

Source: Renesys Path Measurements
Requesting partial disclosure of traffic data

• Disclosure of sufficient amount of traffic data be provided to identify service provider and path of a communication

• Disclosure may be withheld if:
  • Request in relation to political offence
  • Execution of request will prejudice sovereignty, security, ordre public or other essential interests
Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

- Request to another State to search or seize (and disclose) data stored by means of a computer system
  - Located within the territory of the requested State
  - Including data that has been preserved pursuant to Article 29
- [A.23 instruments]
Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

1. A Party may request another Party to search or similarly access, seise or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29

2. (Ability of the requested party to do so)
Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

3. The request shall be responded to on an expedited basis where:

   (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.
Requesting access to stored data

• Request to search, similarly access, seise or similarly secure

• For expedited response:
  • request should have grounds that data is particularly vulnerable to loss or modification

• MLAT and laws should allow for responding on expeditious basis
Article 32 – Transborder Access

• Possibility given to law enforcement from a Party to obtain evidence stored in a computer physically located in other Party’s territory

• Without any request of international cooperation if, during a concrete investigation, the officers in charge
  • need to obtain open source information from a computer located in a foreign country;
  or
  • access data with the lawful and voluntary consent of the lawfully authorised person
A Party may, without the authorisation of another Party:

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

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

- Open source
- Publicly available

G8 Principles on Transborder Access to Stored Computer Data (Moscow 1999)
Public/Open Source Data:

Can be accessed by anyone and used as evidence even though ‘located’ in another country.
Private/Protected Data:

Access restricted to authorised persons (need log-in credentials).
Article 33 - Mutual Assistance Regarding Real Time Collection of Traffic Data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.
Article 34
Mutual assistance regarding the interception of content data

• Mutual assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system

• to the extent permitted under their applicable treaties and domestic laws.
Article 35
24/7 Contact Points

• Obligation to create a permanently available contact point
  • a so called 24/7 network of contact points
• General objectives of these contact points
  • to facilitate international co-operation
  • giving technical advisory to other contact points
  • activating the proper mechanism to expedited preservation of data
  • urgently collecting evidence
  • identifying and discovering suspects
Article 35
24/7 Contact Points

• **Operational network** of experts on high-tech criminality

• Provide **help and cooperation very quickly** even if a formal cooperation request must follow this informal way

• One single point of contact for each country, **available 24 hours a day, 7 days a week**

• **Direct communications between the points**

• Mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide
24/7 Contact Points

• Most contact points are police-based contact points

• Some are Prosecution Services contact points

• Budapest Convention provided a legal basis to the 24/7 network of contact points

• 24/7 networks are recognised as one of the most useful tools regarding international cooperation
MLA request form templates
MANDATORY ASSURANCES

It is confirmed that this request:

(a) does not relate to the prosecution or punishment of a person for a criminal offence that is, or by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character;

(b) is not made for the purposes of prosecuting, punishing or otherwise causing prejudice to a person on account of that person’s race, religion, nationality or political opinions;

(c) does not relate to the prosecution of a person for an offence in a case where the person has been convicted, acquitted or pardoned by a competent court or other authority of (name of requesting place), in respect of that offence or of another offence constituted by the same act or omission as that offence; and

[(d) does not have as its primary purpose the assessment or collection of tax.]11

ASSISTANCE REQUESTED

The Department of Justice of Hong Kong SAR is requested to take such steps as are necessary to give effect to the following:

1. Examination on oath/affirmation of a witness before a magistrate in court.

   (e.g.) Mr. X
   ABC Co., Ltd.
   (address)

   to be orally examined on oath or affirmation on the following matters:

   ● (specify clearly relevant issues/areas relating to subject matter of criminal investigation/prosecution on which evidence of witness is sought and/or provide a list of relevant questions.)

2. Production of things (documents, books etc.) before a magistrate, [and obtaining of oral evidence of the witness producing such material for the purpose of identifying and proving the material produced].12

   (e.g.) Director
   ABC Co., Ltd.
   (address)

   to be required to produce (describe form of evidence e.g. certified copy - the following documents for the period (state relevant time frame)):

   ● (specify documents or classes thereof.)

11 Necessary only if criminal matter is an investigation concerning offences relating to taxation and a bilateral agreement with Hong Kong SAR is in operation.
12 Include this part if deemed necessary for purposes of admissibility of documents in evidence.
MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS
A GUIDE TO IRISH LAW AND PROCEDURES

<table>
<thead>
<tr>
<th>Index</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Central Authority for Mutual Assistance in Criminal Matters</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Requests under International Conventions</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Authorities from which requests may be received</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Form of requests, grounds for refusal and confidentiality (General)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Scope of Irish law on Mutual Legal Assistance in Criminal Matters</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Information about financial transactions for criminal investigation purposes</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Interception of telecommunications messages</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Freezing, Confiscation and Forfeiture of Property</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Provision of Evidence</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Other Forms of Assistance</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Police to police enquiries</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Irish authorities empowered to make requests</td>
<td></td>
</tr>
</tbody>
</table>

5. FORM OF REQUESTS, GROUNDS FOR REFUSAL AND CONFIDENTIALITY - GENERAL

(1) Requests to be addressed to the Central Authority: Requests from designated states must be addressed to the Central Authority, unless the relevant international instrument provides otherwise.

(2) Format of requests: Requests to the Central Authority for mutual legal assistance should be in writing or in any form capable of producing a written record under conditions allowing their authenticity to be established.

(3) Language of requests: All requests and any supporting documents should be in either Irish or English. In cases where requests are not in Irish or English, they must be accompanied by a translation into either of those languages and by a translation of any other such documents or the material parts of them.

(4) Requests to include the fullest information: In general, and subject to the requirements of Irish law set out in this guide and any requirements of the relevant international instrument, requests should contain the fullest information, in particular:

(a) details of the authority making the request, including the name, telephone number and email address (where available) of a contact person

(b) details of the purpose of the request

(c) details of the person or persons named in the request including, where available, address, date of birth and nationality

(d) a description of the offences charged or under investigation

(e) a summary of the facts giving rise to the request

(f) relevant dates e.g. date of court hearing (reason for special urgency or attention should be included in the covering letter of request)

(g) a description of evidence sought, including, in the case of bank accounts, details of the relevant institution, account numbers and account names

(h) specific information on any property to be searched and/or seized

(i) details and supporting documents in relation to the freezing, confiscation or forfeiture of criminal assets
Data Preservation Request

First request: ☐Yes ☐No
Ticket number of the previous request (if available): ....................... 

REQUESTED AUTHORITY

REFERENCE / CASE NUMBER

REQUESTING AUTHORITY

Please be informed that we intend to submit a request for mutual legal assistance to obtain production of the data.

DATE
DD/MM/YYYY

SUBJECT/TITLE

PURPOSE OF THE REQUEST
**URGENCY**

- URGENT

<table>
<thead>
<tr>
<th>Response expected by: DD/MM/YYYY</th>
</tr>
</thead>
</table>

**REASONS FOR URGENCY**

- Threat to life and limb
- Offender in custody
- Crime in progress
- Volatility of data
- Imminent threat of a serious nature to public security
- The only evidence available
- Statute of limitation due to expire
- Other

**DESCRIPTION/JUSTIFICATION FOR URGENCY**

---

**CONFIDENTIALITY**

- The data submitted is only for request purpose
- The data submitted can be used by the requested authority
- The data submitted can be shared with other authorities

---

**OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS**

(Irrespective of their consideration in the requested State)

**OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES**

Choose an item.

**OFFENCES RELATED TO ORGANIZED CRIME AND CORRUPTION**

Choose an item.

**OFFENCES AGAINST THE PERSON**

Choose an item.

**OFFENCES OF FRAUD/FINANCIAL OFFENCES**

Choose an item.

**OTHER SERIOUS OFFENCES**

Choose an item.

**ANY OTHER OFFENCE (PLEASE SPECIFY)**

Choose an item.
### HOW IS THE DATA RELATED TO THE INVESTIGATION

<table>
<thead>
<tr>
<th>APPLYABLE LEGISLATION (SUBSTATIVE AND/OR PROCEDURAL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please cite the most relevant</td>
</tr>
<tr>
<td>Title of Legislation</td>
</tr>
<tr>
<td>Relevant Sections</td>
</tr>
<tr>
<td>Right to Request Data</td>
</tr>
<tr>
<td>Codes of Practice</td>
</tr>
<tr>
<td>Relevant Court Decisions</td>
</tr>
</tbody>
</table>

### CASE STATUS

- [ ] Pre-investigative phase
- [ ] Investigate phase
- [ ] Prosecution phase
- [ ] On trial

Other details: ........................................................................................................................................................................................

### DATA TO BE PRESERVED

- [ ] Subscriber information
- [ ] Traffic data
- [ ] Content data

<table>
<thead>
<tr>
<th>Field</th>
<th>Please specify:</th>
<th>Start date: DD/MM/YYYY</th>
<th>End date: DD/MM/YYYY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period of interest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EXPECTED ANSWERS/RESULTS

- [ ] Confirmation for receiving the request
- [ ] Confirmation for preservation of the data
- [ ] Information of the amount of data preserved
- [ ] Information of the type of data preserved
- [ ] Information on the preservation period
- [ ] Information on legal procedure used for preservation
- [ ] Other: ........................................................................................................................................................................................

### EXPEDITED DISCLOSURE OF PRESERVED TRAFFIC DATA (UNDER ART. 30)

Details:description of data

### REQUESTING AUTHORITY DETAILS

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>Telephone number</td>
<td></td>
</tr>
<tr>
<td>Cell phone number</td>
<td></td>
</tr>
<tr>
<td>E-mail address</td>
<td></td>
</tr>
<tr>
<td>Fax number</td>
<td></td>
</tr>
<tr>
<td>Office Hours</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>

**FOR VERIFICATION BY THE AUTHORISED PERSON, PLEASE CONTACT:**

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Job Title:</td>
</tr>
<tr>
<td>Function:</td>
</tr>
<tr>
<td>Signature:</td>
</tr>
</tbody>
</table>

- Please let us know if, according to this information, you intend to build a criminal case within your country.
- Please let us know if you encounter issues taking into account this request.
- If the system is a shared system, please preserve all basic subscriber information for all virtual systems on the IP.
REQUEST FOR MUTUAL ASSISTANCE REGARDING ACCESSING OF STORED COMPUTER DATA

First request: ☐ Yes ☐ No
Ticket number of the previous request (if available): .....................

REQUESTED AUTHORITY

REFERENCE / CASE NUMBER

REQUESTING AUTHORITY

DATE
DD/MM/YYYY

SUBJECT/TITLE

PURPOSE OF THE REQUEST
URGENCY

☐ URGENT
Response expected by: DD/MM/YYYY

REASONS FOR URGENCY

☐ Threat to life and limb
☐ Offender in custody
☐ Crime in progress
☐ Imminent threat of a serious nature to public security
☐ The only evidence available
☐ Volatility of data
☐ Statute of limitation due to expire
☐ Other:

DESCRIPTION/JUSTIFICATION FOR URGENCY

OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS,
(Irrespective of their consideration in the requested State)

OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES

☐ Illegal Access
☐ Illegal Interception
☐ Data Interference
☐ System Interference
☐ Misuse of devices
☐ Computer-related forgery
☐ Computer-related fraud
☐ Offences related to child pornography
☐ Offences related to infringement of copyright and related rights

OTHER OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS

☐ Terrorism
☐ Sabotage
☐ Murder
☐ Grievous bodily injury
☐ Kidnapping, illegal restraint and hostage-taking
<table>
<thead>
<tr>
<th>Crime Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Racketeering and extortion</td>
</tr>
<tr>
<td>Rape/offences against sexual liberty</td>
</tr>
<tr>
<td>Sexual exploitation of children and child pornography</td>
</tr>
<tr>
<td>Trafficking in human beings</td>
</tr>
<tr>
<td>Illicit trade in human organs and tissue</td>
</tr>
<tr>
<td>Trafficking in stolen vehicles</td>
</tr>
<tr>
<td>Money laundering/Laundering of the proceeds of crime</td>
</tr>
<tr>
<td>Fraud</td>
</tr>
<tr>
<td>Counterfeiting currency</td>
</tr>
<tr>
<td>Forgery of means of payment</td>
</tr>
<tr>
<td>Forgery of documents</td>
</tr>
<tr>
<td>Counterfeiting and piracy of products</td>
</tr>
<tr>
<td>Bribery of national public officials</td>
</tr>
<tr>
<td>Bribery of foreign public officials and officials of public international organizations</td>
</tr>
<tr>
<td>Embezzlement, misappropriation or other diversion of property by a public official</td>
</tr>
<tr>
<td>Trading in influence</td>
</tr>
<tr>
<td>Abuse of functions</td>
</tr>
<tr>
<td>Illicit enrichment</td>
</tr>
<tr>
<td>Bribery in the private sector</td>
</tr>
<tr>
<td>Participation in a criminal organization</td>
</tr>
<tr>
<td>Organised or armed robbery</td>
</tr>
<tr>
<td>Illicit trafficking in narcotic drugs and psychotropic substances</td>
</tr>
<tr>
<td>Illicit trafficking in weapons, munitions and explosives</td>
</tr>
<tr>
<td>Illicit trafficking in cultural goods, including antiques and works of art</td>
</tr>
<tr>
<td>Illicit trafficking in hormonal substances and other growth promoters</td>
</tr>
</tbody>
</table>
### APPLICABLE SUBSTANTIVE LEGISLATION

<table>
<thead>
<tr>
<th>Title of Legislation</th>
<th>Relevant Sections</th>
<th>Right to Request Data</th>
<th>Codes of Practice</th>
<th>Relevant Court Decisions / Confirmation</th>
</tr>
</thead>
</table>

### APPLICABLE PROCEDURAL LEGISLATION TO BE FOLLOWED IN THE OBTAINING OF EVIDENCE

<table>
<thead>
<tr>
<th>Title of Legislation</th>
<th>Relevant Sections</th>
<th>Right to Request Data</th>
<th>Codes of Practice</th>
<th>Relevant Court Decisions / Confirmation</th>
</tr>
</thead>
</table>

### CASE STATUS

- [ ] Pre-investigative phase
- [ ] Investigate phase
- [ ] Prosecution phase
- [ ] On trial

Other details: ____________________________________________________________
..................................................................................................................

### SUBSCRIBER INFORMATION

#### Period of Interest

<table>
<thead>
<tr>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
</table>

#### Data specification

- [ ] Subscriber names
- [ ] User names
- [ ] Screen names, or other identities
- [ ] Mailing addresses
- [ ] Residential addresses
- [ ] Business addresses
<table>
<thead>
<tr>
<th><strong>Data Types</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email addresses</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Telephone numbers, other contact information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Billing records</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Billing address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Payment method</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Payment History</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Billing period</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Information about length of service and the types of services the subscriber(s) or customer(s) used</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Any other identifying information, whether such records are in electronic or other form</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Connection logs and records of user activity for the subscriber(s) identified above, including log-in history and records identifying sent and received communications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>All communications stored in the account(s) of the subscriber(s) identified above</strong></td>
<td></td>
</tr>
<tr>
<td><strong>All files that are controlled by user accounts associated with the subscriber(s) identified above</strong></td>
<td></td>
</tr>
</tbody>
</table>

| **Name, username and postal address of the holder of the account** | |

| **Name, username and postal address of the holder of the account** | |
| **When was the account registered?** | **DD/MM/YYYY** |
| **Is the account still active?** | |

### USER DATA

| **Service ID (Skype, Windows Live, Chat room, etc.)** | |
| **Social Networking Service ID (Facebook, etc.)** | |
| **IP address used for the initial registration of the account** | |
| **IP address used for the last registered access to the account** | |
| **IP address used for access to the account on** | **Date:** DD/MM/YYYY  **Time:** |
| **IP address used for sending message from the account** | |
| **Message details:** | **Date:** DD/MM/YYYY  **Time:** |
| **Other relevant data** | |
**TRAFFIC DATA**

**Accessed IP address / range of IP addresses**

<table>
<thead>
<tr>
<th>IPv4</th>
<th>1-255</th>
<th>1-255</th>
<th>1-255</th>
</tr>
</thead>
</table>

**Date**

<table>
<thead>
<tr>
<th>Time Zone</th>
</tr>
</thead>
</table>

**IPv6 Address**

<table>
<thead>
<tr>
<th>Subnet – 64 bit</th>
<th>Host – 64 bit</th>
</tr>
</thead>
</table>

**Date**

<table>
<thead>
<tr>
<th>Time Zone</th>
</tr>
</thead>
</table>

**E-mail Address Specification**

<table>
<thead>
<tr>
<th>E-mail address</th>
<th>@</th>
</tr>
</thead>
</table>

**Date**

<table>
<thead>
<tr>
<th>Time</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Zone Time</th>
</tr>
</thead>
</table>

**Person/Organisation details**

<table>
<thead>
<tr>
<th>Business Name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Legal Name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Contact name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Country</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>E-mail</th>
</tr>
</thead>
</table>

**CONTENT DATA**

- Electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files

- Deleted files, cache files, user information, and other
<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail and other data</td>
<td></td>
</tr>
<tr>
<td>All operating systems, software, applications, hardware, operating manuals, codes, keys and other support information</td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

**Origin of the data (if known)**

**Destination of the data (if known)**

**Other relevant details**

**Actions Requested in Relation to Data**

**Requesting Authority Details**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Telephone number</td>
</tr>
<tr>
<td>Cell phone number</td>
</tr>
<tr>
<td>E-mail address</td>
</tr>
<tr>
<td>Fax number</td>
</tr>
<tr>
<td>Office Hours</td>
</tr>
<tr>
<td>Time Zone</td>
</tr>
</tbody>
</table>

**For Verification by the Authorised Person, Please Contact:**

<table>
<thead>
<tr>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title:</td>
</tr>
<tr>
<td>Function:</td>
</tr>
<tr>
<td>Signature:</td>
</tr>
</tbody>
</table>
What affects International Cooperation
What affects International Cooperation
Bear in mind possible differences

Legal System
- Common law
- Civil Law
- Hybrid
- Islamic law

Different powers & functions same name
- Prosecutors/police

Different codes of procedure
- Custody deadlines
- Powers to enter, search and seize
- Surveillance powers (technical & physical)
What affects International Cooperation?

Making requests:

- Legal Basis
- Domestic procedures (Bureaucracy/getting permission)
- Don’t know who to contact
- Don’t know how to make a request
- Don’t know what can request
- Don’t know how to write a request
- Lack of capacity and resources
- Politics
- Language
What affects International Cooperation?

Receiving requests:

- Legal Basis
- Domestic procedures (Bureaucracy/getting permission)
- Lack of capacity and resources
- Politics
- Language
What affects International Cooperation?

- Trust
- Capacity
- Skills
- Funding
- Culture
- Politics
- Legal Structure
- Speed
- Time
- Attribution
Trust

- Leaks
- Don’t want to share credit
- Past failures
- Poor standards
- Unknown quantity
- Perception follow rules
- Good Structures
- Understood system & procedures
- Previous Good Experience
- Perceived as trustworthy
- Similar Background
Capacity

- Procedures exist to process a request
- Sufficient staff to process request
- Legally allowed to obtain evidence
- Appropriate forensic tools to process the data
- Appropriate equipment available (e.g. Faraday bags; secure storage)
Skills

- Forensic specialists skilled in the area of investigation requested
- Specialist knowledge to request correct and appropriate analysis
- Know how to fill in the request to appropriate legal standard
- Competence in language of request
Funding

- Forensic specialists remain properly trained and retained
- Able to purchase software licences
- Able to pay any 3rd party charges
  - ISP costs
  - Defence Attorney fees
  - Translation
- Able to pay for storage and secure transport of evidence
Culture

- Is there a cooperation mindset?
- Has cooperation existed previously?
- Prepared to share the credit?
- Does hierarchy accept that impossible to go it alone?
Politics

- Do the countries have a working relationship?
- Do those that authorise cooperation accept such a relationship is desirable?
- Are there other political issues that could work against cooperation?
Legal Structures

- Is the dual criminality principle satisfied?
- Are the countries signatories to an appropriate legal instrument?
- Are the domestic laws and procedures in place?
- Do they work well enough?
Electronic evidence inherent challenges:

- Identify and locate the evidence
- Secure the hardware
- Capture and analyse the data
- Maintain integrity and chain of custody
- Comply with rules of court and admissibility
- Link the suspect to use of the device at the relevant time (‘Attribution’)

In final analysis, these are your aims:

International cooperation should support and facilitate them
Questions