

# Data preservation vs. data retention: Data protection perspective in criminal investigations

Mick Jameison MSc CNE



**Project Cybercrime@EAP III**  
*Public/private cooperation*

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Տարգ տաղփաղսլի Parteneriat  
Oriental Усходняе Партнёрства

# Data retention.

Protection of privacy

“Saying that you don’t care about the right to



have nothing to say.”

Jean-Michel Jarre.

Fight against terrorism and crime.

“I think privacy is



you don't have anything to hide.”

Ashton Kutcher

**Project Cybercrime@EAP III**  
*Public/private cooperation*

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Ֆարգ տərəfdaşlığı Partenariat  
Oriental Усходняе Партнёрства

# Data Retention Considerations

- Data Retention – EU Directive 2006/24/EC
  - Telecom and ISPs data retention 6 – 24 months
- Annulment of EU Directive 2006/24/EC in 2014
  - Invalid for violating rights of privacy
- UK still seeks to compel organisations such as ISP to retain data.
  - LEA can only be authorised to gain access to stored material.
- Note – Data Retention is not mentioned in the Budapest Convention.

# Why do some the LEA agencies believe data retention is useful?

- Criminals develop, they don't start as experts.
- Criminals learn from their mistakes.
- Criminals learn about anonymisation.
- Anonymity tools improve.
- Detection and identification skills improve.
- Sometimes the answer maybe in the past.



# How was Silk Road's Ross Ulbricht identified.

- Linked in profile.
- Connections to a nickname called, "Altoid."
- IP connections to VPN Server for Silk Road
- Made a mistake in making a historic posting using his real Google email address.



The image shows a LinkedIn profile for Ross Ulbricht, an Investment Adviser and Entrepreneur in the Austin, Texas Area. His previous education is listed as Pennsylvania State University. Below the profile is a blue 'Connect' button and a notification of 106 connections. Underneath is a large green advertisement for 'Silk Road anonymous marketplace' featuring a camel logo. At the bottom is a screenshot of the Silk Road website interface, showing a search bar and a list of items for sale, including 'Cocaine Energy Drink - Banned'.

#### altoid:

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro i the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. En environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

If interested, please send your answers to the following questions to [rossulbricht@gmail.com](mailto:rossulbricht@gmail.com)

# With so many sites, who is the next major criminal administrator?

The screenshot shows a forum interface with a dark blue theme. At the top left is the 'GW' logo. The top right shows a user profile for 'UserNan' with 1000 messages and a registration date of January 01. Below the header is a navigation bar with links for 'Форум ссылки', 'Search', 'Members', and 'Calendar'. A login status bar indicates 'Logged in as: Forgetaboutit (Log Out)'. A search bar is located below the login bar. The main content area features several advertisements, including one for 'Track 1 | VISA classic \$8 | EU A' and another for 'SE-CODE'. Below the ads is a forum listing table with columns for 'Forum', 'Topics', 'Replies', and 'Last Post Info'. The table lists several forums, including 'Русский Общий Форум' and 'Forum for Russian'. At the bottom of the screenshot, a portion of an email inbox is visible, showing messages from 'Just skimmed FRESH dumps' and 'PlasticPower email Update'.

Family Cards (CW)

Logged in as: Forgetaboutit (Log Out)

Глобальный поиск по статусу, имени, icq, e-mail

Умные люди здесь делают бабки!!!

www.CardingWorld.cc

Forum	Topics	Replies	Last Post Info
Русский Общий Форум Все последние сообщения, отправленные в русских форумах, вы можете видеть здесь	21.218	94.661	Today, 20:30 In: Protected Forum By: panchbob
Кардинг Все темы, касающиеся кардинга. Forum Led by: David@	319	3.068	Today, 00:24 In: нововведения ) By: Maranello
Новости в мире кардинга Новости, касающиеся кардинга, взятые из открытых источников Forum Led by: UpLevel, David@, Xenon	644	2.265	Today, 17:32 In: Почему русские хакеры лучшие... By: Voland.
Безопасность для кардеров	100	1.000	Today, 08:16

Just skimmed FRESH dumps  
сарас 2007-03-...

PlasticPower email Update  
plasticpower 2007-03-...

Quality IE EXPLOIT for low price! 2007-03-...

# Expedited preservation of stored computer data. Articles 16 – 19

- 16 - Expedited preservation of stored computer data.
- 17 - Expedited preservation and partial disclosure of traffic data.
- 18 - Production order.
- 19 - Search and seizure of stored computer data.
- What do these mean in practice in an investigation?

# Case Study - emails





# London Arrests.

- Fraud identified at Stagebeat.
- sibna22@yahoo.com
  - Preservation request  
14<sup>th</sup> July
- 78 Albatross Close,  
London. UK



# London arrests – Search 15<sup>th</sup> July

- Two prisoners.
- Five computers containing over 800 card details.
- Forged identification documents.
- On-line fraud.



**Project Cybercrime@EAP III**  
**Public/private cooperation**

Արևելյան Գործընկերության  
Տվյալները  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Ֆորդ տաբփաճկի Parteneriat  
Oriental Усходняе Партнёрства

# London Arrests – e-mails

- Preservation requests on e-mails on 14<sup>th</sup> - 17<sup>th</sup> July after arrests and examination of computers.
- E-mails received from Yahoo - USA 23<sup>rd</sup> April following year.
- Vietnamese suspects e-mail accounts (204,000 credit cards) – **mattfeuter@gmail.com**
- Egyptian suspects e-mail accounts (18,000 credit cards) – **menem99@gmail.com**



**Project Cybercrime@EAP III**  
*Public/private cooperation*

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Տեղեկատվական Բարենախ  
Oriental Усходняе Партнёрства

# Prosecution examining e-mails

## Data Protection challenges

- Legal privilege.
- Unread emails – is this interception?
- Collateral intrusion.
- Irrelevant emails – retention or not?
- Intelligence sharing – in compliance with court production order or not.
- Secure storage of material.
- Retention time period.
- Service on defence solicitors (with many defendants)



**Project Cybercrime@EAP III**  
***Public/private cooperation***

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Տարբ տաբժաճկի Partenariat  
Oriental Усходняе Партнёрства

# London Arrests - Prisoners

- Gboyega AKINBOLA.
- AKA – sibna22, lopey14,
- Oyetunde OYEDEJI.
- AKA – teedazzles, candidman, lopey14
- Subsequently sentenced to two and half years imprisonment.



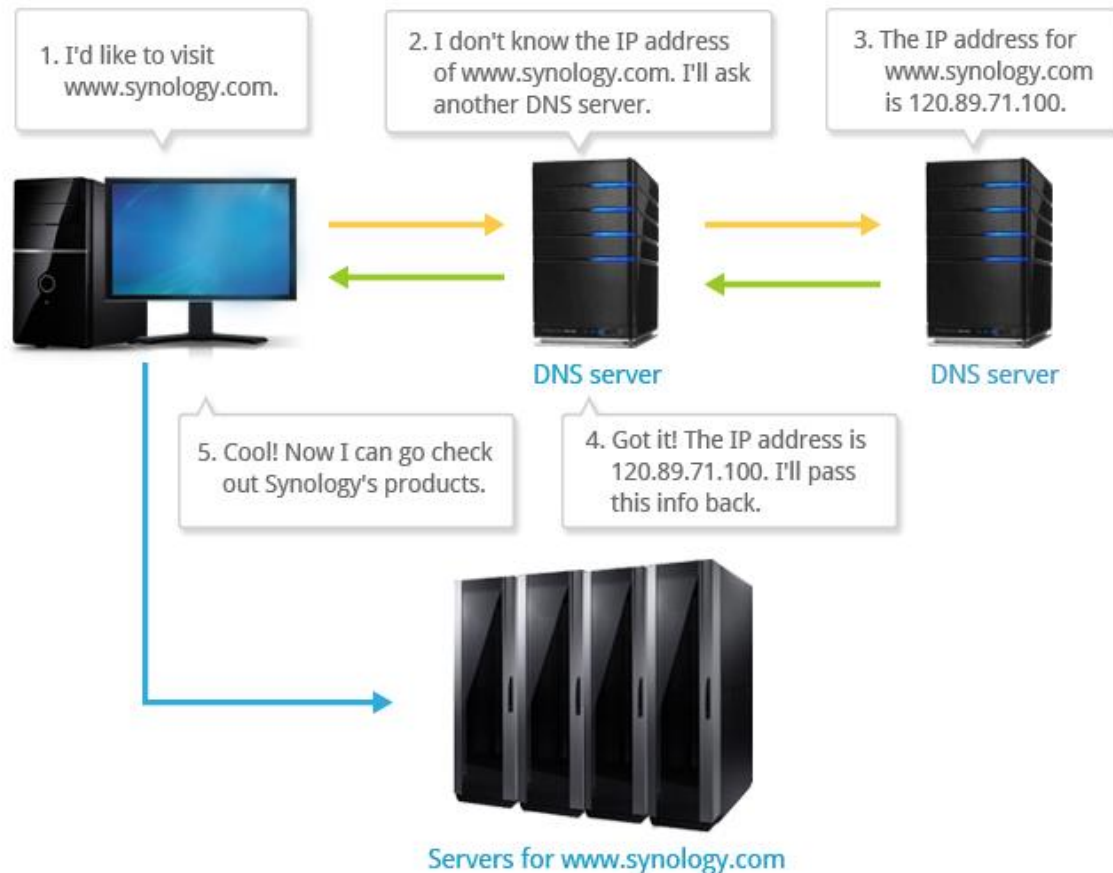
**Project Cybercrime@EAP III**  
***Public/private cooperation***

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Ֆարգ տərəfdaşlığı Partenariat  
Oriental Усходняе Партнёрства

# Case Study - Website



# Locating a website server?



# Intellectual Property Investigation

The screenshot displays a web browser window with the address bar showing 'Sean Paul | RnBExclusive'. The website header includes the 'RNB XCLUSIVE' logo and a navigation menu with links for HOME, DOWNLOADS, EXCLUSIVES, VIDEOS, ADVERTISE, and CONTACT. A search bar is located on the right side of the header. The main content area features a large image of Sean Paul with a red mohawk and green sunglasses, with the text 'SEAN PAUL TOMAHAWK TECHNIQUE' overlaid. To the right of the main content, there is a sidebar with a 'Follow' button, a Facebook widget, a 'Subscribe' button, and a 'CATEGORIES' list. The browser's address bar shows 'Sean Paul | RnBExclusive'.



# Preservation requests

Website

DNS



**Project Cybercrime@EAP III**  
*Public/private cooperation*

Արևելյան Գործընկերության  
Տիմը  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Տարբերակային Parteneriat  
Oriental Усходняе Партнёрства

# MLAT requests

## Website

- The HDD or a certified copy.
- Payment records.
- Communication with site owner(s).

## DNS

Payment records.  
How long will DNS be off line for?  
Are there any connected DNS

# Prosecution examining website Data Protection challenges

- IP Connection history – how do we deal with this.
- Legal privilege.
- Collateral intrusion.
- eMail accounts on servers.
- Intelligence sharing – in compliance with court production order or not.
- Secure storage of material.
- Retention time period.
- Service on defence solicitors (paper versions are not normally possible).

# The future may involve more arguments about jurisdiction and privacy.

## Microsoft, Facebook, Google and Yahoo release US surveillance requests

- Tech giants turn over data from tens of thousands of accounts
- Limited disclosure part of transparency deal made last month

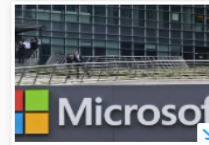


Microsoft, Twitter, Google and Facebook all participate in the NSA's Prism effort. Photograph: Pichi Chuang/Reuters

Tens of thousands of accounts associated with customers of Microsoft, Google, Facebook and Yahoo have their data turned over to US government authorities every six months as the result of secret court orders, the tech giants disclosed for the first time on Monday.

## Microsoft wins appeal over U.S. email requests

Elizabeth Weise, USATODAY Published 12:14 p.m. ET July 14, 2016 | Updated 6:08 p.m. ET July 14, 2016



(Photo: Michel Euler, Associated Press)

CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

SAN FRANCISCO — In a ruling that has important data security implications, a court ruled Thursday Microsoft can't be forced to give the government e-mails stored in Ireland that are part of a U.S. drug investigation.

DISRUPT SF Prices increase on Disrupt SF tickets in less than 24 hours Grab your tickets now & save

government

Federal Bureau of Investigation

law

warrants

Government

Popular Posts



Swift creator Chris Latner joins Google Brain after Tesla Autopilot stint 3 days ago



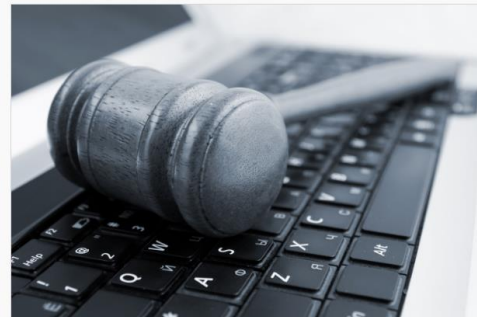
Amazon's private label business is booming thanks to device sales, expanded fashion lines 2 days ago



A defense company put a machine gun on a drone

## Google told to hand over foreign emails in FBI search warrant ruling


Posted Feb 4, 2017 by Natasha Lomas (@riptari)



A U.S. judge has ordered Google to hand over emails stored outside the country in order to comply with an FBI search warrant. The warrant in question pertains to a domestic fraud probe.

# Thank you.

Mick Jameison MSc CNE



**Project Cybercrime@EAP III**  
***Public/private cooperation***

Արևելյան Գործընկերության  
Східне партнерство Eastern  
Partnership აღმოსავლეთ  
პარტნიორობა Parteneriatul  
Estic Տեղական տեղական  
Oriental Усходняе Партнёрства