FRIEND OR FOE?

Whom to Trust in a World of PRISM, XKeyscore and related Programs.

Harald Reisinger

Managing Director (Research & Development) of RadarServices GmbH

ABOUT HARALD REISINGER

- University of Economics at Vienna, University of Nebraska at Omaha (USA)

- IT-Security Industry since 2001

- Certified Information Security Manager, ISO 27001 Lead Auditor

- Managing Director Research & Development of RadarServices GmbH

ABOUT RADARSERVICES GMBH

- Providing continuous IT-Riskmanagement Services

- Unique service-approach by combining automated risk detection and human risk evaluation

- Combining different views on potential risk (Vulnerabilities, Network Anomalies, SIEM, System Changes, Compliance etc.)

- Headquarter in Austria, Branches in Poland, Russia and UAE (Dubai)
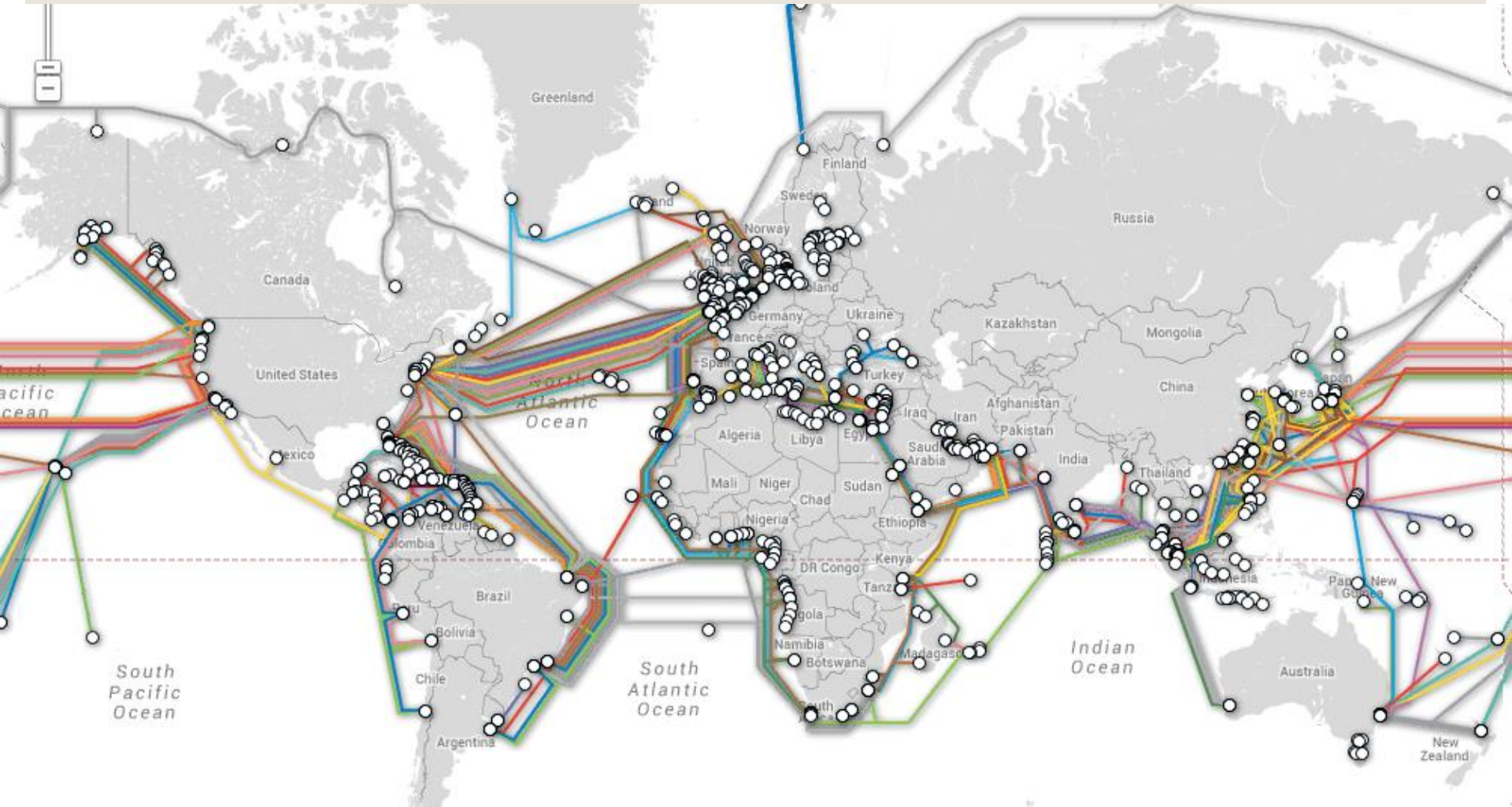
Trust

Whom to trust?

IN A CONNECTED WORLD…

GLOBAL TRAFFIC MAP 2010

THROUGH 880.000 KM OF SEA-CABLE...

**We,
the good guys**

**Them,
the bad guys**

Then, there was May 2013.

US$ 52.600.000.000,00
Black Budget for US Intelligence in 2013

Of these
US$ 52.600.000.000,00

$$\vee$$

US$ 11.000.000.000,00
for Consolidated Cryptology Program

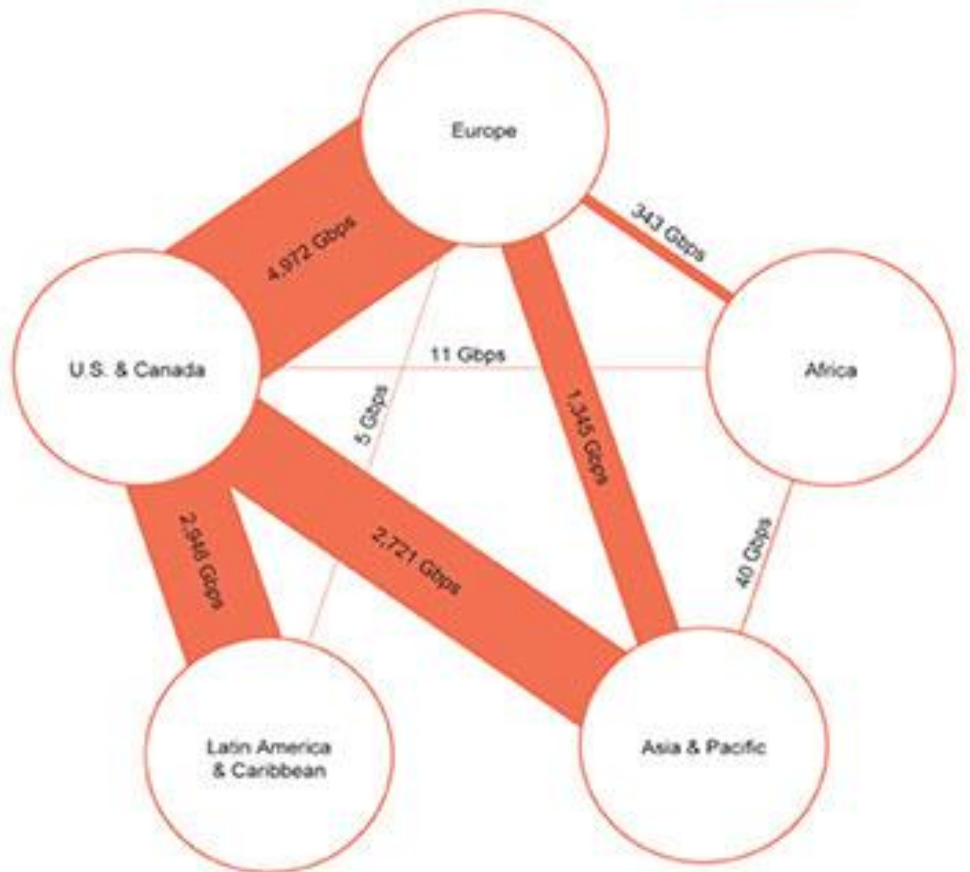# 107.035 Employees

+

21.800 Contractors

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- Much of the world's communications flow through the U.S.

- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.

- Your target's communications could easily be flowing into and through the U.S.

Europe

U.S. & Canada

Africa

Latin America & Caribbean

Asia & Pacific

4,972 Gbps

343 Gbps

11 Gbps

5 Gbps

1,345 Gbps

2,948 Gbps

2,721 Gbps

40 Gbps

International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

Microsoft 9/11/07

Yahoo 3/12/08

Google 1/14/09

Facebook 6/3/09

PalTalk 12/7/09

YouTube 9/24/10

Skype 2/6/11

AOL 3/31/11

Apple (added Oct 2012)

2007   2008   2009   2010   2011   2012   2013
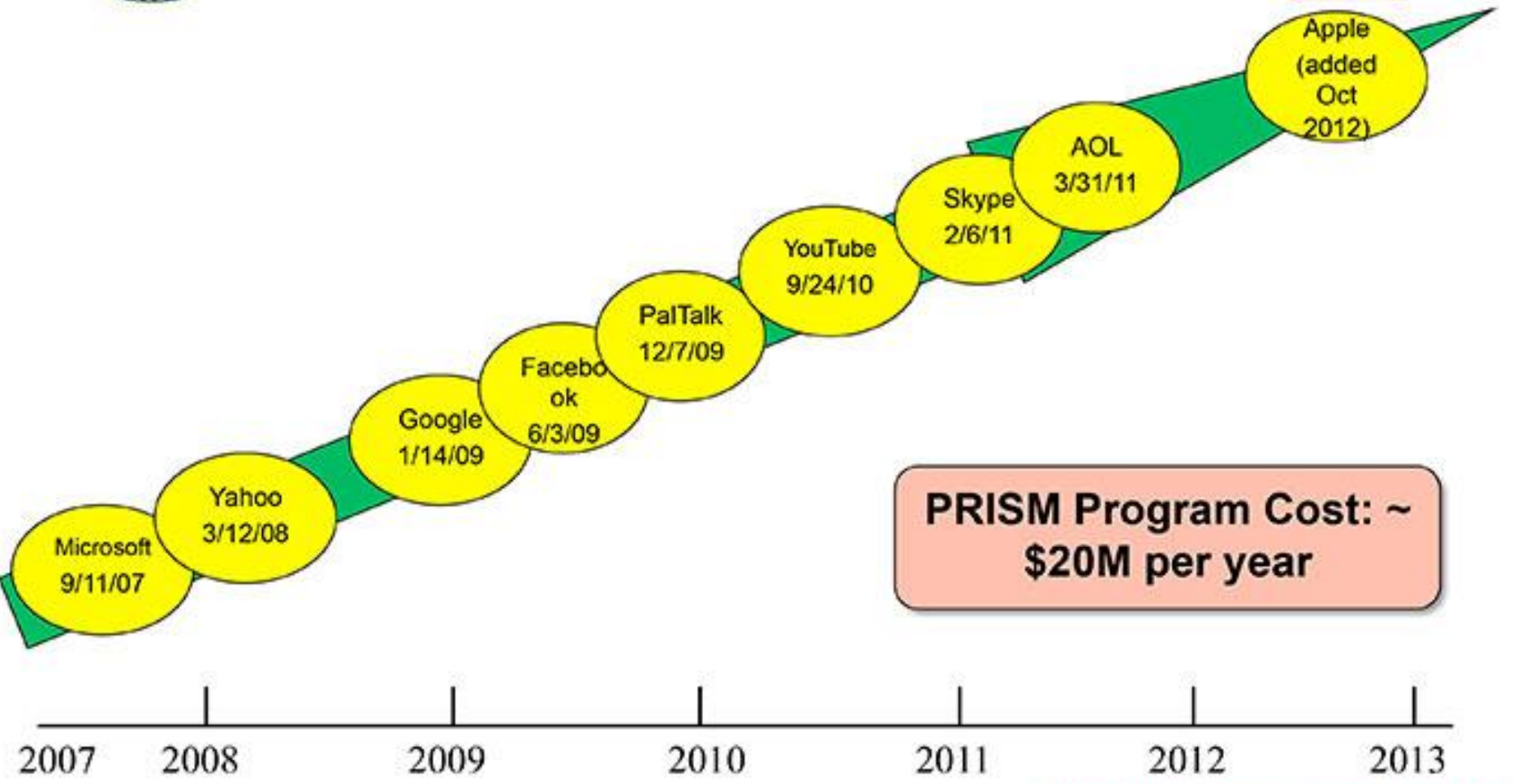
(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
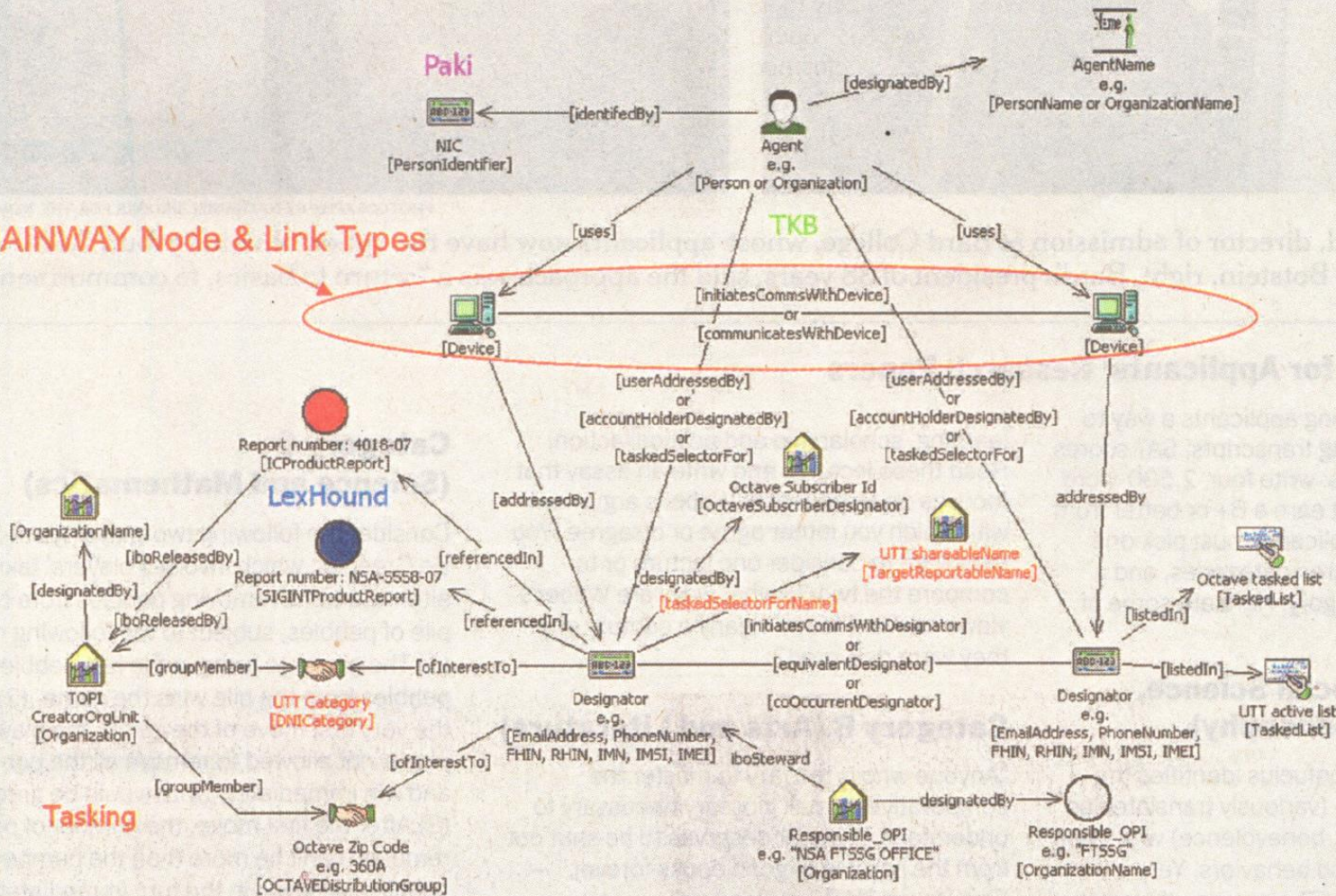- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

(S//SI//REL USA, FVEY) SYANPSE Data Model

CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Paki

AgentName
e.g.
[PersonName or OrganizationName]

[designatedBy]

[identifedBy]

NIC
[PersonIdentifier]

Agent
e.g.
[Person or Organization]

[uses]   **TKB**   [uses]

MAINWAY Node & Link Types

[initiatesCommsWithDevice]
or
[communicatesWithDevice]

[Device]   [Device]

[userAddressedBy]   [userAddressedBy]
or   or
[accountHolderDesignatedBy]   [accountHolderDesignatedBy]
or   or
[taskedSelectorFor]   [taskedSelectorFor]

Report number: 4016-07
[ICProductReport]

LexHound

[addressedBy]   Octave Subscriber Id   addressedBy
                       [OctaveSubscriberDesignator]

[OrganizationName]

[iboReleasedBy]   [referencedIn]   **UTT sharsableName**
                                                    [TargetReportableName]   Octave tasked list
[designatedBy]   [TaskedList]
                                          [designatedBy]
Report number: NSA-5558-07
[SIGINTProductReport]   **[taskedSelectorForName]**

[iboReleasedBy]   [referencedIn]   [initiatesCommsWithDesignator]   [listedIn]
                                                     or
[groupMember]   [ofInterestTo]   [equivalentDesignator]   [listedIn]
TOPI   or
CreatorOrgUnit   [coOccurrentDesignator]
[Organization]   **UTT Category**   UTT active list
                        [DNICategory]   Designator   Designator   [TaskedList]
                                              e.g.   e.g.
                                              [EmailAddress, PhoneNumber,   [EmailAddress, PhoneNumber,
                        [ofInterestTo]   FHIN, RHIN, IMN, IMSI, IMEI] FHIN, RHIN, IMN, IMSI, IMEI]
[groupMember]   iboSteward

Tasking
                                                                  designatedBy
Octave Zip Code
e.g. 360A   Responsible_OPI   Responsible_OPI
[OCTAVEDistributionGroup]   e.g. "NSA FTSSG OFFICE"   e.g. "FTSSG"
                                            [Organization]   [OrganizationName]

THE NEW WAY   *BOUNDLESSINFORMANT*

(U//FOUO) Use Big Data technology to query SIGINT collection in the cloud to produce near real-time business intelligence describing the agency's available SIGINT infrastructure and coverage.

(U//FOUO) Key Questions

1. How many records are collected for an organizational unit (e.g. FORNSAT) or country?

2. Are there any visible trends?

3. What assets collect against a specific country? What type of collection?

4. What is the field of view for a specific site? What type of collection?

(U//FOUO) Potential Users

1. Strategic decision makers (leadership team)

2. Tactical users (mission and collection managers)

BUILDING AND PUSHING AN INDUSTRY

- Bridge between US Government / US Intelligence Agencies and US Corporations is blurring
- Brain and Money flow into Ventures
- More that US$ 1 Bill. of Early Stage Funding into IT-Security in Silicon Valley in 2012

In-Q-Tel

ArcSight
An HP Company

FireEye®

In-Q-Tel

platfora

mongoDB

huddle

WE LIKE TO PROVIDE DATA

- 84% of all Search Traffic is US-controlled

- The Worlds most widely used Social Platforms are US-based

- „That's cool!" beats „Do they care?"

Android

Full access to WLAN passwords

Full access to stored files

Full access to iMessages

TECHS TOP INNOVATORS ARE US-BASED

#	2013
1	facebook
2	workday
3	Linked in
4	skype
5	GROUPON
6	(Twitter logo)
7	servicenow
8	paloalto NETWORKS
9	360buy.com 京东商城
10	zynga

9 out of 10 (2013 listing)

Patriot Act
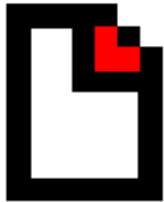
Lavabit

My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.

Lavabit

My Fellow Users.

> "…This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States."

American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.

Storing and processing huge amount of data

Area of Stasi filing cabinets

200 "file-kilometers" correspond
to about 48'000 filing cabinets
which use up about 0.019 km².

zoom in

Area of NSA filing cabinets

5 Zettabytes printed out
equate to about 42 trillion filing cabinets
which would use up about 17 Mio. km².

start zooming out

1984

WAS NOT
SUPPOSED
TO BE AN
INSTRUCTION
MANUAL

MOTIVATION FOR DATA GATHERING

- Prevent Money Laundring
- Prevent Terrorism
- Old-fashioned Intelligence Tasks
- Business

MOTIVATION FOR DATA GATHERING

- ✅ Prevent Money Laundring
- ✅ Prevent Terrorism
- ✅ Old-fashioned Intelligence Tasks
- Business ❓

It's the Economy, Stupid!

BUSINESS DRIVERS

- Collect competitive information
- Generate intellectual property
- Push GDP
- Brain drain to US

504 Mill.

316 Mill.

🇪🇺 **12,8 Trill. €**

🇺🇸 **11,8 Trill. €**

Steps to take...

EUROPEAN UNION / GOVERNMENTS

- Invest in People, Education and Innovation
- Encourage Start-Ups in promising Industries
- Provide extensive Seed and Venture Capital
- Provide flexible Pan-European Business Context

BUYERS

- Buy European Technology and Services
- Take Steps to Protect Corporate Assets
- Reconsider usage of Cloud Services
- Enforce and use Open Encryption Standards
- Enhance Awareness for Topic

IT-COMPANIES

- Don't follow, take the Lead!
- Team up
- Consider Europe as one Market
- Be Proud and Pushy!

So: Whom to Trust now?

Thank you!