What THEY Know, What YOU Don't:
Digital Intrusion & Digital Privacy

St. Louis UNIX Users Group

Scott Granneman
Denise Lieberman

© 2013 R. Scott Granneman
Last updated 20130911
You are free to use this work, with certain restrictions.
For full licensing information, please see the last slide/page.

?

!

Scott

ABOUT WUSTL

Leadership

Facts, History and Traditions

Campus Stores

About St. Louis

Logos, Symbols & Marks

Print & Digital Media

Commencement

Technology

Compliance & Policies

Visitors, Tours & Maps

The mission of Washington University in St. Louis is the promotion of learning — learning by students and by faculty. Teaching, the transmission of knowledge, is central to our mission, as is research, the creation of new knowledge.

Faculty — composed of scholars, scientists, artists and members of the learned professions — serve society by teaching; by adding to the store of human art, creativity, understanding, and wisdom; and by providing direct services, such as health care.

The university offers more than 90 programs and almost 1,500 courses leading to bachelor's, master's and doctoral degrees in a broad spectrum of traditional and interdisciplinary fields, with additional opportunities for minor concentrations and individualized programs.

Brookings Hall
Washington University's signature building

Washington University in St. Louis

Technology in Our Changing Society

Technology for Managers

Web Development
& Advanced Web Development

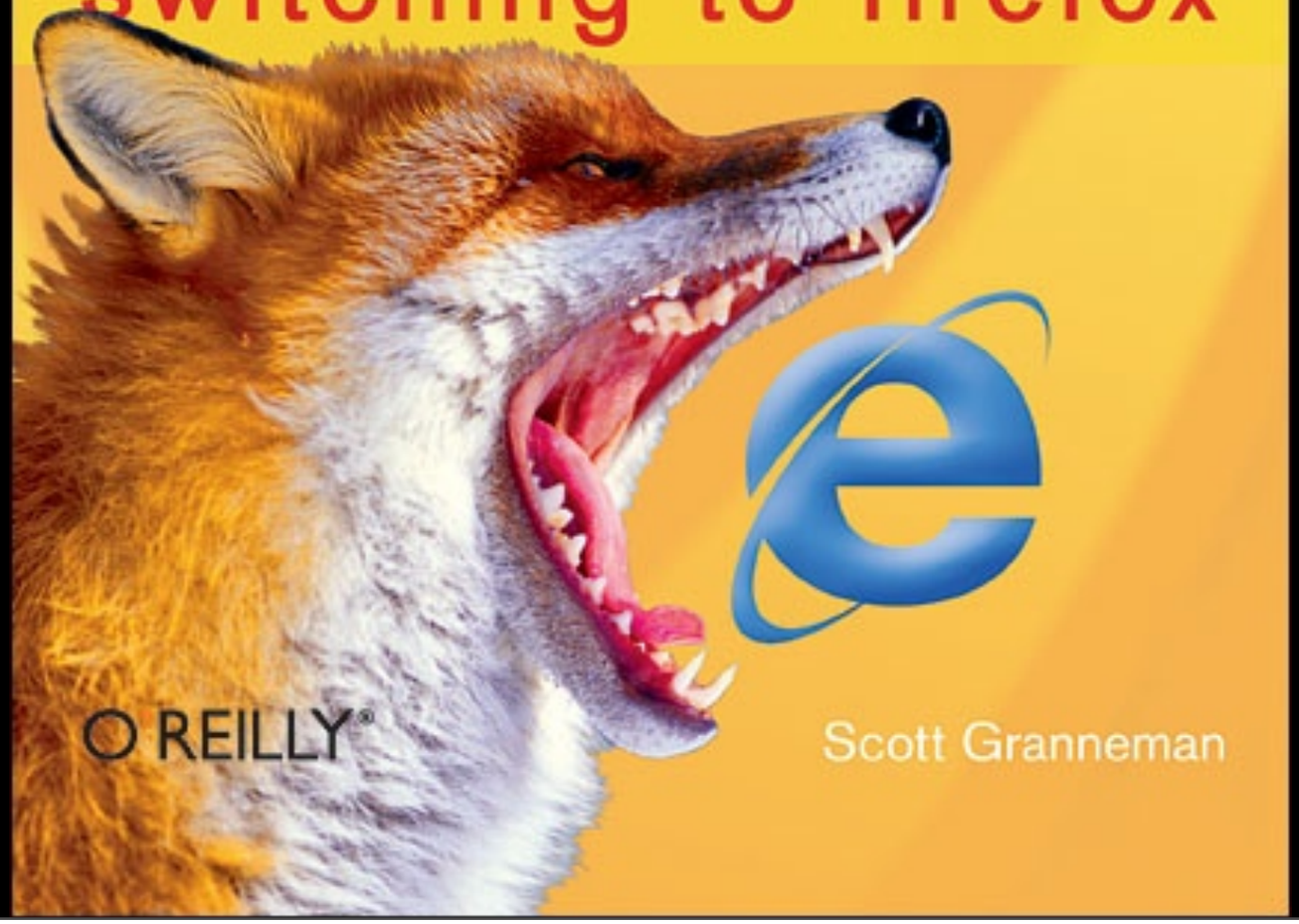
From Blogs to Wikis:
Building Community
in a Virtual Environment

Technology & the Law

Practical Security

don't click on the blue e!

switching to firefox



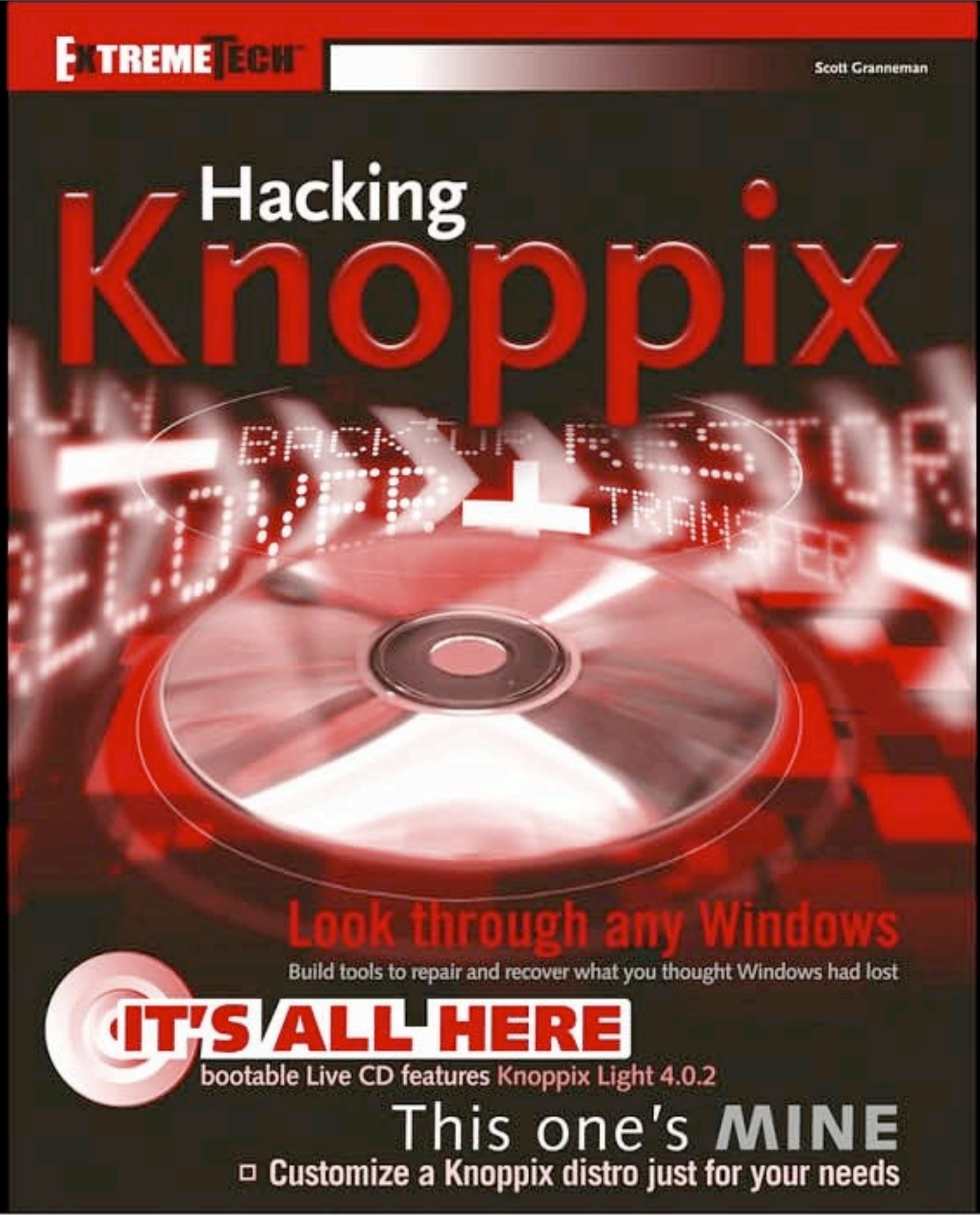
O REILLY®

Scott Granneman

EXTREMETECH

Scott Granneman

Hacking Knoppix



Look through any Windows

Build tools to repair and recover what you thought Windows had lost

IT'S ALL HERE

bootable Live CD features Knoppix Light 4.0.2

This one's MINE

- Customize a Knoppix distro just for your needs

Scott Granneman

ESSENTIAL CODE AND COMMANDS

Linux®

PHRASEBOOK

shortcut

Your Short Cut to Knowledge

Podcasting with Audacity™

Creating a Podcast with Free Audio Software

Mac, Windows, and Linux

Dominic Mazzoni and Scott Granneman

SOURCEFORGE

Community Press

www.prenhallprofessional.com

Audacity

PRENTICE HALL

NEGUS SOFTWARE SOLUTIONS SERIES

Google™ Apps

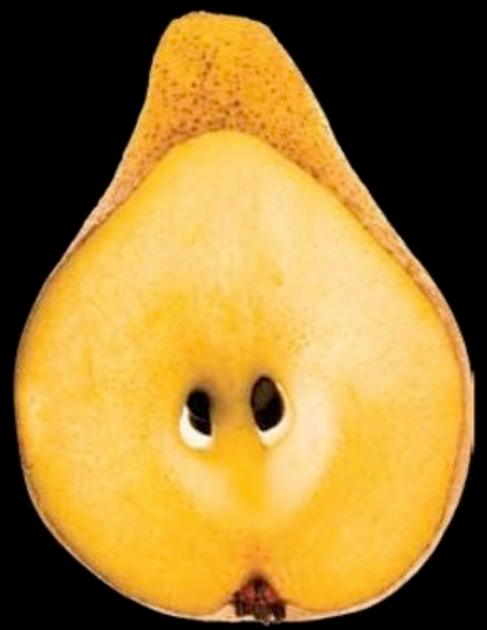
DECIPHERED

Compute in the Cloud to Streamline Your Desktop

Scott Granneman

PRACTICE SOFTWARE FREEDOM

Mac and iPhone book for
users and developers



Mac OS X Snow Leopard for Power Users

Advanced Capabilities and Techniques

Scott Granneman

Apress®

Browsers, phishing, and user interface design - Mozilla Firefox <2>

File Edit View Go Bookmarks Tools Help

Back

http://www.securityfocus.com/columnists/405

Go

Browsers, phishing, and user int...1

SecurityFocus™

About Advertising Contact

Symantec ThreatCon

Level 2: Elevated

2

Threat level definition

Home | Bugtraq | Vulnerabilities | Mailing Lists | Tools | Search: SEARCH

News

Infocus

- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Columnists

Mailing Lists

- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics

PRINT EMAIL COMMENT (page 1 of 2) next

Browsers, phishing, and user interface design

Scott Granneman, 2006-06-05

Phishing works for so many reasons, we need to rethink browser and user interface design to provide some real-life security to the average user who doesn't see or understand the security cues.

Occasionally a criminal is so, well, clever that you have to admire him even as you wish that he spends the rest of his life in jail. Take Arnold Rothstein, for instance. One of the kingpins of organized crime in New York City during Prohibition and before, the "Great Brain," as he was termed, was more than likely behind the infamous Black Sox scandal, in which the 1919 World Series was fixed in favor of the Cincinnati Reds. He is also widely credited with inventing the floating crap game immortalized in *Guys and Dolls*. Like some character out of a Damon Runyon story, Rothstein's "office" was outside of Lindy's Restaurant, at Broadway and 49th Street, and he

" Answer me this truthfully: do you really trust Aunt Sally or Steve in Accounting or your kid sister Brooke to carefully read an anti-phishing warning, ponder the ramifications, and then make a wise choice? If you answer in the affirmative, then you haven't read Why Phishing Works. "

Scott Granneman

Done 2.517s 5 Errors PageRank Alexa

DECEMBER 2005 LINUX MAGAZINE Interview with Marten Mickos • MySQL 5 • Wireless USB Volume 7 / Issue 12

LINUX MAGAZINE

OPEN SOURCE. OPEN STANDARDS.

THE MYSQL DATABASE LEAPS AHEAD

INTERVIEW WITH MÅRTEN MICKOS

The MySQL AB CEO on Open Source, Staying Competitive

APPLICATION DEVELOPMENT WITH MYSQL 5

Coding with Triggers, Views, and Stored Procedures

PERIPHERALS UNBOUND

Wireless USB Banishes Cables

ALSO INSIDE:

- Debug Perl Like a Pro
- OpenDocument Upends Microsoft
- Go Fish: The Friendly Interactive Shell

DECEMBER 2005

WWW.LINUXMAGAZINE.COM

WebSanity - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Back http://www.websanity.com/ Go

WebSanity

Home Philosophy Experience Methodology Disciplines Solutions contact

Design for a Better World

WebSanity provides user-centric Web design solutions, with a focus on working with non-profit organizations, including:

- Web Design, Planning and Consulting
  - Content Management Systems
  - E-commerce
  - Online Membership and Marketing
  - Online Multimedia & Interactive Interpretives

Successful Web design and development is more than meets the eye. Our proven process helps ensure you get the most out of your Web site, regardless of how large or small your organization is.

This site is designed as an introduction not only to what we do, but best Web development practices in general.

© 2003 WebSanity!

Done 3.584s PageRank Alexa

Washington University in St. Louis • School of Medicine

Department of Neurology

Diocese of Missouri
THE EPISCOPAL CHURCH

Pokémon

Saint Louis Zoo

geochemical society

ACLU
AMERICAN CIVIL LIBERTIES UNION of NEW JERSEY

CHARIS
The St. Louis Women's Chorus

ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

ACLU
AMERICAN CIVIL LIBERTIES UNION of MINNESOTA

ACLU
AMERICAN CIVIL LIBERTIES UNION of SOUTH CAROLINA

ACLU
AMERICAN CIVIL LIBERTIES UNION of PENNSYLVANIA

ACLU
AMERICAN CIVIL LIBERTIES UNION of EASTERN MISSOURI

ACLU
AMERICAN CIVIL LIBERTIES UNION of CONNECTICUT

Denise

Senior Attorney, 2006–Present

Washington University in St. Louis

Courts & Civil Liberties

National Security, Civil Liberties & the Law

Gender & Law

Sexuality & Law

Technology & the Law

Legal Director of ACLU-EM
1997-2005

Technology
never gets worse.
It only gets better.

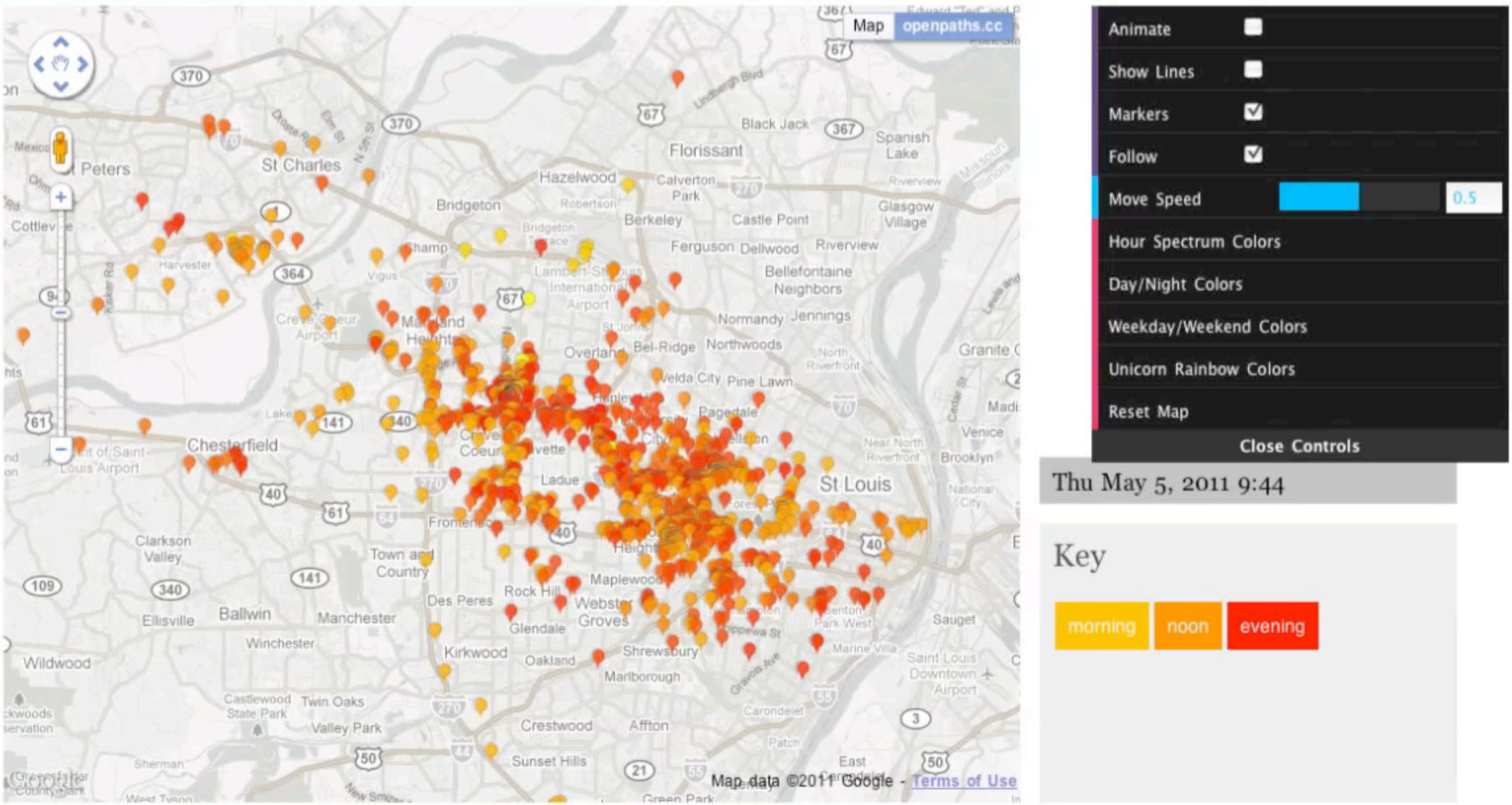
Bruce Schneier

You have zero privacy anyway.
Get over it.

Scott McNealy,
SUN, 1999

Any unencrypted message
sent over the Internet
is being delivered
to every intelligence service
in the world.

Edward Snowden,
August 13, 2013


Map
openpaths.cc
Animate
Show Lines
Markers
Follow
Move Speed
0.5
Hour Spectrum Colors
Day/Night Colors
Weekday/Weekend Colors
Unicorn Rainbow Colors
Reset Map
Close Controls
Thu May 5, 2011 9:44
Key
morning
noon
evening
Map data ©2011 Google - Terms of Use

ATLANTA
·BREAD·
COMPANY
BAKERY CAFE
intel Inside
pentium 4
Designed for
Microsoft
Windows XP

What's a *packet sniffer*?

A program and/or device that monitors the data passing through a network

✓ Where data is coming from

✓ Where data is going

✓ What the data is

www.wireshark.org

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: imap contains LOGIN | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
392	46.193576	66.39.82.33	192.168.2.111	IMAP	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS AUTH=LOGIN] g
395	46.254800	66.39.82.33	192.168.2.111	IMAP	Response: * CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY U
396	46.260155	192.168.2.111	66.39.82.33	IMAP	Request: 1 LOGIN "[redacted]" "[redacted]"

Frame 396 (98 bytes on wire, 98 bytes captured)

Ethernet II, Src: 00:02:2d:2b:e7:34, Dst: 00:0f:3d:84:d4:37

Internet Protocol, Src Addr: 192.168.2.111 (192.168.2.111), Dst Addr: 66.39.82.33 (66.39.82.33)

Transmission Control Protocol, Src Port: 50527 (50527), Dst Port: imap2 (143), Seq: 15, Ack: 371, Len: 32

Internet Message Access Protocol

```
0000  00 0f 3d 84 d4 37 00 02  2d 2b e7 34 08 00 45 00   ..=..7.. -+.4..E.
0010  00 54 fc 1e 40 00 40 06  e7 25 c0 a8 02 6f 42 27   .T..@.@. .%...oB'
0020  52 21 c5 5f 00 8f 90 7f  de ed f1 34 df ce 80 18   R!._.... ...4....
0030  07 cc cd 8f 00 00 01 01  08 0a 00 29 23 9d 8e 64   ........ ...)#..d
0040  5f 10 31 20 4c 4f 47 49  4e 20 22 73 63 6f 74 74   _.1 LOGI N "[redacted]
0050  22 20 22 5c 5c 30 37 29  69 4f 54 61 26 5c 5c 22   " "[redacted]"
0060  0d 0a                                             ..
```

File: (Untitled) 1185 KB 00:01:51 Drops: 0 | P: 1711 D: 3 M: 0

Sunday, October 6, 13

20100511.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http contains facebook | Expression... | Clear | Apply

No. .	Time	Source	Destination	Protocol	Info
13	6.294614	192.168.1.114	66.220.145.13	HTTP	GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1
168	106.564880	192.168.1.114	69.63.176.174	HTTP	GET /x/3806658556/false/p_504568267=3 HTTP/1.1
364	272.187522	192.168.1.114	69.63.176.174	HTTP	GET /x/2004290339/false/p_504568267=3 HTTP/1.1
4334	298.940663	192.168.1.139	66.220.145.35	HTTP	GET /p HTTP/1.1
4336	299.056349	192.168.1.139	66.220.145.35	HTTP	GET /x/1262269691/false/p_1158900097=29 HTTP/1.1
4349	299.223074	192.168.1.139	69.63.189.34	HTTP	GET /ajax/presence/reconnect.php?__a=1&reason=0&iframe_loaded=t
4432	299.514930	192.168.1.139	66.220.145.35	HTTP	GET /x/3366637175/false/p_1158900097=0 HTTP/1.1
4433	299.515794	192.168.1.139	66.220.145.35	HTTP	[TCP Out-Of-Order] GET /x/3366637175/false/p_1158900097=0 HTTP/
4444	299.732803	192.168.1.139	69.63.189.34	HTTP	POST /ajax/chat/buddy_list.php?__a=1 HTTP/1.1 (application/x-w
4760	302.490790	192.168.1.139	69.63.189.34	HTTP	GET /ajax/chat/history.php?__a=1&id=1348823550 HTTP/1.1
5088	305.877586	192.168.1.114	69.63.189.31	HTTP	GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1
6639	324.403128	192.168.1.139	77.67.87.122	HTTP	GET /hprofile-ak-sf2p/hs649.snc3/27486_100000479785789_586_q.jp
7053	335.333305	192.168.1.139	77.67.87.122	HTTP	GET /hprofile-ak-sf2p/hs309.ash1/23244_883125579_9824_q.jpg HTT

```
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    X-SVN-Rev: 244938\r\n
    Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439\r\n
    [truncated] Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87; datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c4
    \r\n
```

```
01b0  35 39 2d 31 2c 75 74 66  2d 38 3b 71 3d 30 2e 37   59-1,utf -8;q=0.7
01c0  2c 2a 3b 71 3d 30 2e 37  0d 0a 4b 65 65 70 2d 41   ,*;q=0.7 ..Keep-A
01d0  6c 69 76 65 3a 20 31 31  35 0d 0a 43 6f 6e 6e 65   live: 11 5..Conne
01e0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
01f0  65 0d 0a 58 2d 53 56 4e  2d 52 65 76 3a 20 32 34   e..X-SVN -Rev: 24
0200  34 39 33 38 0d 0a 52 65  66 65 72 65 72 3a 20 68   4938..Re ferer: h
0210  74 74 70 3a 2f 2f 77 77  77 2e 66 61 63 65 62 6f   ttp://ww w.facebo
0220  6f 6b 2e 63 6f 6d 2f 70  72 6f 66 69 6c 65 2e 70   ok.com/p rofile.p
0230  68 70 3f 69 64 3d 35 30  34 35 36 38 32 36 37 26   hp?id=50 4568267&
0240  76 3d 77 61 6c 6c 26 73  74 6f 72 79 5f 66 62 69   v=wall&s tory_fbi
0250  64 3d 31 31 38 33 38 34  38 33 34 38 36 31 34 33   d=118384 83486143
0260  39 0d 0a 43 6f 6f 6b 69  65 3a 20 5f 5f 75 74 6d   9..Cooki e: __utm
0270  61 3d 38 37 32 38 36 31  35 39 2e 31 33 31 36 31   a=872861 59.13161
0280  39 33 33 36 38 2e 31 32  32 36 30 31 30 37 30 39   93368.12 26010709
0290  2e 31 32 35 37 36 33 30  31 32 36 2e 31 32 35 37   .1257630 126.1257
```

HTTP Referer (http.referer),... | Packets: 52773 Displayed: 133 Marked: 0 | Profile: Default

20100511.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http contains facebook | Expression... | Clear | Apply

No. .	Time	Source	Destination	Protocol	Info
13	6.294614	192.168.1.114	66.220.145.13	HTTP	GET /ajax/intent.php?_a=1&filter=h&pending=true&request_type=1
168	106.564880	192.168.1.114	69.63.176.174		e/p_504568267=3 HTTP/1.1
364	272.187522	192.168.1.114	69.63.176.174		e/p_504568267=3 HTTP/1.1
4334	298.940663	192.168.1.139	66.220.145.35		
4336	299.056349	192.168.1.139	66.220.145.35		e/p_1158900097=29 HTTP/1.1
4349	299.223074	192.168.1.139	69.63.189.34		onnect.php?__a=1&reason=0&iframe_loaded=t
4432	299.514930	192.168.1.139	66.220.145.35		e/p_1158900097=0 HTTP/1.1
4433	299.515794	192.168.1.139	66.220.145.35		/x/3366637175/false/p_1158900097=0 HTTP/
4444	299.732803	192.168.1.139	69.63.189.34		list.php?__a=1 HTTP/1.1 (application/x-w
4760	302.490790	192.168.1.139	69.63.189.34		.php?__a=1&id=1348823550 HTTP/1.1
5088	305.877586	192.168.1.114	69.63.189.31		_a=1&filter=h&pending=true&request_type=1
6639	324.403128	192.168.1.139	77.67.87.122		hs649.snc3/27486_100000479785789_586_q.jp
7053	335.333305	192.168.1.139	77.67.87.122		hs309.ash1/23244_883125579_9824_q.jpg HTT

```
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
X-SVN-Rev: 244938\r\n
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_
[truncated] Cookie: __utma=87286159.1316193368.1226010709.1257630126.1
\r\n
```

ad27950d744d1218866ad8da792d7b1eb02acc1c

```
0000  00 21 29 c8 71 84 00 1f  5b d0 be 27 08 00 45 00   .!).q... [..'..E.
0010  04 cf 51 22 40 00 40 06  4f 03 c0 a8 01 72 42 dc   ..Q"@.@. O....rB.
0020  91 0d e8 25 00 50 a8 01  8d a8 55 fa 64 2e 80 18   ...%.P.. ..U.d...
0030  ff ff 7b af 00 00 01 01  08 0a 2e 40 90 e4 89 1b   ..{..... ...@....
0040  8d f1 47 45 54 20 2f 61  6a 61 78 2f 69 6e 74 65   ..GET /a jax/inte
0050  6e 74 2e 70 68 70 3f 5f  5f 61 3d 31 26 66 69 6c   nt.php?_ _a=1&fil
0060  74 65 72 3d 68 26 70 65  6e 64 69 6e 67 3d 74 72   ter=h&pe nding=tr
0070  75 65 26 72 65 71 75 65  73 74 5f 74 79 70 65 3d   ue&reque st_type=
0080  31 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   1 HTTP/1 .1..Host
0090  3a 20 77 77 77 2e 66 61  63 65 62 6f 6f 6b 2e 63   : www.fa cebook.c
00a0  6f 6d 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   om..User -Agent:
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 4d 61 63   Mozilla/ 5.0 (Mac
00c0  69 6e 74 6f 73 68 3b 20  55 3b 20 49 6e 74 65 6c   intosh;  U; Intel
00d0  20 4d 61 63 20 4f 53 20  58 20 31 30 2e 35 3b 20    Mac OS  X 10.5;
```

Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window

Ready to load or capture | Packets: 52773 Displayed: 133 Marked: 0 | Profile: Default

Sunday, October 6, 13

Follow TCP Stream

Stream Content

```
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=hExjWSXqWGyly5VASXeUeQ; lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fref%
3Dlogo%23%2Fprofile.php%3Fid%3D504568267%26v%3Dwall%26story_fbid%3D118384834861439;
presence=DJ273608322G14H0L504568267A3BF2736083251l0WMblcMsndPBbloMbvtP273590669BctP273604456BsbPBtA_7bQBuctP273608321BsA0QBblADacA29V27360
8222Z284BlcPBcvrADrA0.96BtsP273588495QQQ; cur_max_lag=2; e=n

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k..........I.....W..!
.,...!D5...d.k.z.x..2.gv!..0.......|."..+.
... S....e.......b..+..M....~B..-......>.6..tEu,..f..K/.._z...2w...a.....Q...#6..t..0.$......r.......l..
.......K..w.p..,.......a(........].>
```

Find | Save As | Print | Entire conversation (10512 bytes) | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ◉ Raw

Help | Filter Out This Stream | Close

Follow TCP Stream

Stream Content

```
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=hExjWSXqWGyly5VASXeUeQ; lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fref%
3Dlogo%23%2Fprofile.php%3Fid%3D504568267%26v%3Dwall%26story_fbid%3D118384834861439;
presence=DJ273608322G14H0L504568267A3BF273608325110WMblcMsndPBbloMbvtP273590669BctP273604456BsbPBtA_7bQBuctP273608321BsA0QBblADacA29V27360
8222Z284BlcPBcvrADrA0.96BtsP273588495QQQ; cur_max_lag=2; e=n

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k..........I.....W..!
.,...!D5...d.k.z.x..2.gv!..0.......|."..+.
... S....e.......b..+..M....~B..-......>.6..tEu,..f..K/.._z...2w...a.....Q...#6..t..0.$......r.......l..
.......K..w.p..,.......a(........].>
```

Find | Save As | Print | Entire conversation (10512 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

Follow TCP Stream

Stream Content

```
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=hExjWSXqWGyly5VASXeUeQ; lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fref%
3Dlogo%23%2Fprofile.php%3Fid%3D504568267%26v%3Dwall%26story_fbid%3D118384834861439;
presence=DJ273608322G14H0L504568267A3BF273608325110WMblcMsndPBbloMbvtP273590669BctP273604456BsbPBtA_7bQBuctP273608321BsA0QBblADacA29V27360
8222Z284BlcPBcvrADrA0.96BtsP273588495QQQ; cur_max_lag=2; e=n

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k..........I.....W..!
.,...!D5...d.k.z.x..2.gv!..0.......|."..+.
... S....e.......b..+..M....~B..-......>.6..tEu,..f..K/.._z...2w...a.....Q...#6..t..0.$......r.......l..
.......K..w.p..,.......a(........].>
```

Find | Save As | Print | Entire conversation (10512 bytes) | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ◉ Raw

Help | Filter Out This Stream | Close

Follow TCP Stream

Stream Content

```
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87;
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=hExjWSXqWGyly5VASXeUeQ; lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fref%
3Dlogo%23%2Fprofile.php%3Fid%3D504568267%26v%3Dwall%26story_fbid%3D118384834861439;
presence=DJ273608322G14H0L504568267A3BF273608325110WMblcMsndPBbloMbvtP273590669BctP273604456BsbPBtA_7bQBuctP273608321BsA0QBblADacA29V27360
8222Z284BlcPBcvrADrA0.96BtsP273588495QQQ; cur_max_lag=2; e=n

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k..........I.....W..!
.,...!D5...d.k.z.x..2.gv!..0.......|."..+.
... S....e.......b..+..M....~B..-......>.6..tEu,..f..K/.._z...2w...a.....Q...#6..t..0.$......r.......l..
.......K..w.p..,.......a(........].>
```

Find | Save As | Print | Entire conversation (10512 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

Follow TCP Stream

Stream Content

```
GET /ajax/intent.php?__a=1&filter=h&pending=true&request_type=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 244938
Referer: http://www.facebook.com/profile.php?id=504568267&v=wall&story_fbid=118384834861439
Cookie: __utma=87286159.1316193368.1226010709.1257630126.1257734728.87
datr=1233161259-6735bad27950d744d1218866ad8da792d7b1eb02acc1c44d0580c; lxe=yunicornechu%40yahoo.com; xs=6937dd979d5f3e2ae4e4ae22912f65c9;
lo=hExjWSXqWGyly5VASXeUeQ; lxr=1; locale=en_US; c_user=504568267; sct=1272591608; sid=3; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fref%
3Dlogo%23%2Fprofile.php%3Fid%3D504568267%26v%3Dwall%26story_fbid%3D118384834861439;
presence=DJ273608322G14H0L504568267A3BF2736083251l0WMblcMsndPBbloMbvtP273590669BctP273604456BsbPBtA_7bQBuctP273608321BsA0QBblADacA29V27360
8222Z284BlcPBcvrADrA0.96BtsP273588495QQQ; cur_max_lag=2; e=n

[12968 bytes missing in capture file]Ys....x.....
m..Z.......ek.-!
J*%.k..........I.....W..!
.,...!D5...d.k.z.x..2.gv!..0.......|."..+.
... S....e.......b..+..M....~B..-......>.6..tEu,..f..K/.._z...2w...a.....Q...#6..t..0.$......r.......l..
.......K..w.p..,.......a(........].>
```

Find | Save As | Print | Entire conversation (10512 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

View Photos of Kathryn (936)
View Videos of Kathryn (3)
Send Kathryn a Message

And when things start to happen, don't worry. Don't stew. Just go right along. You'll start happening too.

Information

Networks:
Washington University in St. Louis '09
Vanderbilt Grad Student '12

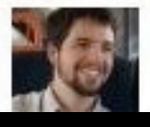
Relationship Status:
Married to
Rebecca Estee

Birthday:
November 25, 1986

Current City:
Saint Louis, MO

Friends

464 friends See All



Kathryn Austin

Add as Friend

Wall Info

Kathryn only shares some of her profile information with everyone. If you know Kathryn, send her a message or add her as a friend.

About Me

Basic Info

Sex:	Female
Birthday:	November 25, 1986
Siblings:	Jay Austin
Parents:	Gene Austin
Relationship Status:	Married to Rebecca Estee
Anniversary:	August 20, 2005
Current City:	Saint Louis, Missouri
Hometown:	Austin, Texas
Religious Views:	everything and nothing, including but not limited to: DDR

Bio

There is always a reason to celebrate.

Favorite Quotations

How very special are we,
for just a moment to be,
part of life's eternal rhyme,
how very special are we,
to have on our family tree,
Mother Earth and Father Time.
-Charlotte's Web

Work and Education

Grad School

Vanderbilt University '12 M.Ed.

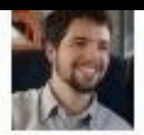
Create an Ad

St Louis Bucket List
Things to do in St Louis before you die. One huge coupon emailed daily.
Like

Aspiring Photographer?
Earn your degree 100% online. Over 40 courses to choose from. Request FREE Information Today!
Like

Self-Publish Your Book
New book design, editing & marketing programs available to help you successfully self-publish. Click for 555 free book promotion tips.
Like

More Ads


Raymond Colletti

Mario Treto Jr.

Tony Renner

Amy Trummer

Andy Doy

Jennifer Serendipitous Minkowitz

Report/Block this Person

Share

Work and Education

Grad School — **Vanderbilt University '12** M.Ed.
Human Development Counseling

College — **Washington University in St. Louis '09**

High School — **Westlake High School '05**

Likes and Interests

Activities — Mentoring, Singing, Geocaching

Mentoring

Interests — Complexity, Simplicity

Complexity

Music — More Fools than Wise, The Bright Light Social Hour, Beastpower

More Fools than Wise

Books — Oh, the Places You'll Go!

Oh, the Places You'll Go!

Television — SpongeBob SquarePants, Degrassi

SpongeBob SquarePants

Show other Pages

Chat (43)

Report/Block this Person

Share

Activities	Mentoring, Singing, Geocaching	Mentoring
Interests	Complexity, Simplicity	Complexity
Music	More Fools than Wise, The Bright Light Social Hour, Beastpower	More Fools than Wise
Books	Oh, the Places You'll Go!	Oh, the Places You'll Go!
Television	SpongeBob SquarePants, Degrassi	SpongeBob SquarePants

Show other Pages

Contact Information

Contact Info	Mobile Number:	5126951475
	Website:	http://fools.wustl.edu
	Facebook Profile:	http://www.facebook.com/austin.kathryn

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NATIONAL SECURITY
AGENCY

June 6, 2013

theguardian

The Washington Post

NSA Prism program taps in to user data of Apple, Google and others

June 6, 2013

the guardian

The Washington Post

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

PRISM enables
“collection directly from the servers”
of online companies

(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:

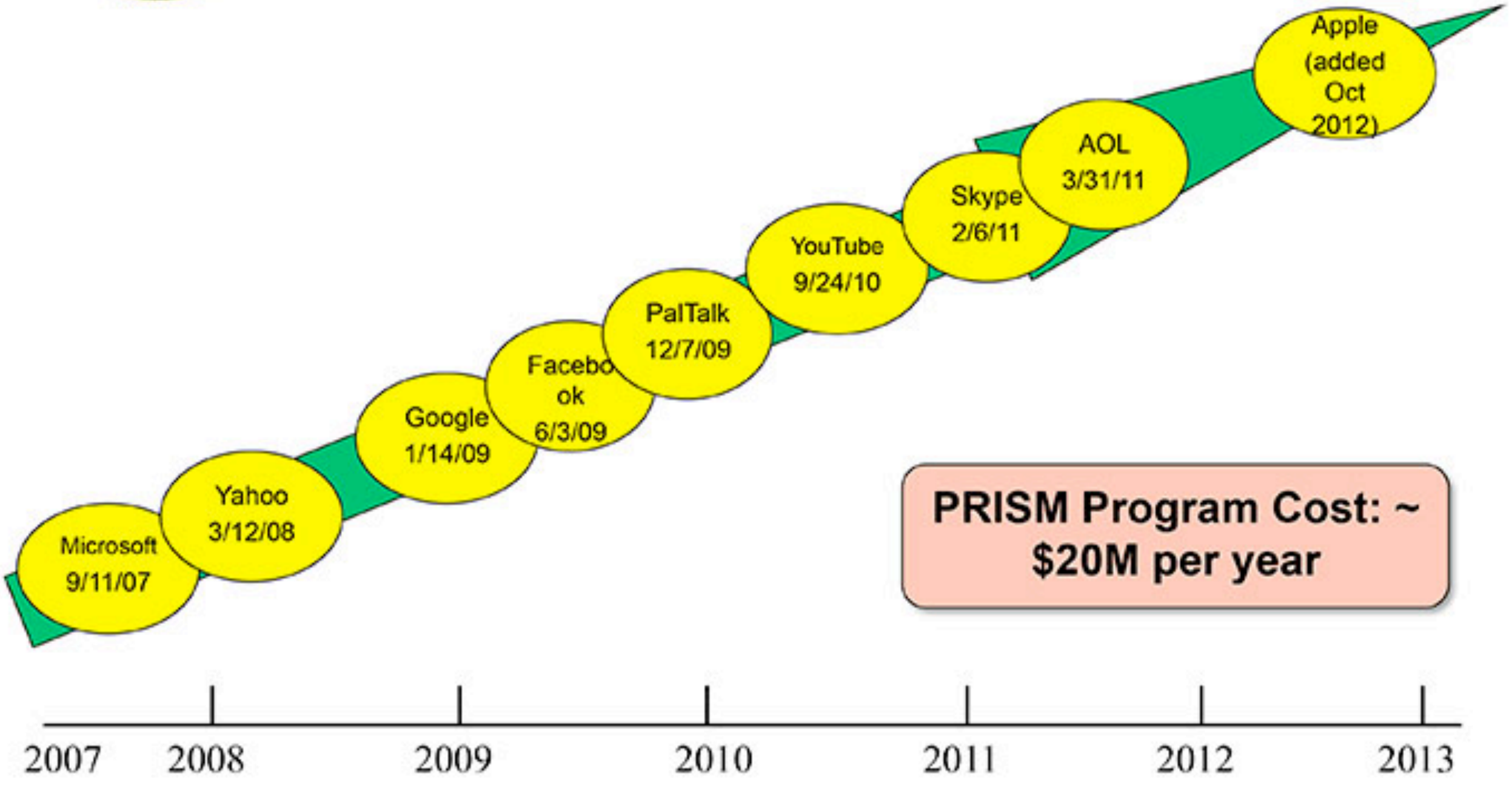
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

“extensive, in-depth surveillance
on live communications
and stored information”

Can acquire communications
that were encrypted
while traveling over the Internet
once they’re on servers

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



“98 percent of PRISM production is based on Yahoo, Google and Microsoft”

Accounts for 91%
of NSA's Internet traffic
acquired under FISA § 702

Available to low-level NSA analysts

No court approvals needed

Don’t need supervisor approval

Must ignore US citizen's data
if analyst is at least 51% sure
he's American

Training materials say
analysts should periodically report
accidental collection of citizen data,
but if they do collect it,
"it's nothing to worry about"

July 17, 2013

John C. Inglis, Deputy Director, NSA

NSA analysts can perform
“a second or third hop query”
through data

Hop 1
A suspect’s contacts

↓

Hop 2
Hop 1’s contacts

↓

Hop 3
Hop 2’s contacts

2011

University of Milan researchers
calculate that on average
everyone on the Internet is
4.74 steps away
from anyone else

Assuming the average person
calls 40 people,
a 3-hop analysis allows the NSA
to mine data on 2.5 M Americans
when investigating 1 suspect

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

June 6, 2013

theguardian

The top secret rules that allow NSA to use US data without a warrant

Secret FISA Court documents
show that data gathered
about U.S. citizens
must be destroyed

Secret FISA Court documents
show that data gathered
about U.S. citizens
must be destroyed

… unless circumstances exist
in which it can be
collected, retained, & used

NSA can store
“inadvertently acquired”
domestic communications
if they contain:

✓ Foreign intelligence information
✓ Evidence of a crime
✓ Threats of serious harm
✓ Encrypted communications
✓ Any other information
that could aid
the NSA’s electronic surveillance

June 29, July 9, August 31, September 9

theguardian

DER SPIEGEL

O GLOBO

Who has the NSA been spying on?

NSA spied on …

France
Italy
Greece
Japan
Mexico
South Korea
India
Turkey
Mexico
Venezuela
Colombia
Ecuador
Argentina
Panama
Costa Rica
Nicaragua
Honduras
Paraguay
Chile
Peru
El Salvador

As well as …

Google

Brazilian oil company
Petrobras

Al Jazeera
Media Network

Saudi Arabia’s
Riyad Bank

Chinese tech company
Huawei

French Ministry of
Foreign Affairs

Society for Worldwide
Interbank Financial
Telecommunication
(SWIFT)

International Atomic
Energy Agency

European Union
embassy

United Nations

In addition, NSA spied on …

✓ Brazilian president Dilma Rousseff
✓ Mexican president Peña Nieto
(then a candidate)

NSA sought information on:

Oil, energy, & trade
Corporate espionage

September 5, 2013

ProPublica

theguardian

The New York Times

Revealed: how US and UK spy agencies defeat internet privacy and security

September 5, 2013

PRO PUBLICA

theguardian

The New York Times

Feds Beg NY Times, Pro Publica Not To Reveal That They've Inserted Backdoors Into Internet Encryption

from the *too-fucking-bad* dept

Hacker News commenter:

“My takeaway from today’s articles:
they’ve backdoored the software,
they’ve backdoored the hardware,
they have a database
of stolen private keys,
they’ve tapped all the cables,
they have zero-days
for pretty much everything.”

https://news.ycombinator.com/item?id=6338365

September 7, 2013

DER SPIEGEL

Privacy Scandal: NSA Can Spy on Smart Phone Data

Operating systems

✓ BlackBerry
✓ iPhone
✓ Android

Data

✓ Contact lists
✓ SMS traffic
✓ Notes
✓ Location information

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) …that this would be big brother...

TS//SI//REL to USA, FVEY

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...and the zombies would be paying customers?

TS//SI//REL to USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

(U) Post Processed BES collection

#	Type	Data Type	Source	Destination
	BlackBerry - CMIME	Plaintext		

EMAIL | CONTROL | HEADER | C2C | KEYWORDS | CONTENTMETA | DECODED_TEXT | COMMENTS (0)

From: [redacted]
To: [redacted]
Subject: RE: URGENTE: Sorteo del SEM

Email Body | **BlackBerry - CMIME**

S69843880 **2098E117**

-----Mensaje original-----
De: [redacted]
Enviado el: [redacted]
Para: [redacted]
Asunto: RE: URGENTE: [redacted]

[redacted]

Gracias,

TOP SECRET//COMINT//REL TO USA, FVEY

September 11, 2013

theguardian

NSA shares raw intelligence including Americans' data with Israel

- Secret deal places no legal limits on use of data by Israelis
- Only official US government communications protected
- Agency insists it complies with rules governing privacy

September 11, 2013

theguardian

The NSA is sharing data with Israel. Before filtering out Americans' information.

NSA sends Israel “Raw Sigint”:

“unevaluated and unminimized transcripts, gists, facsimiles, telex, voice and Digital Network Intelligence metadata and content.”

NSA does not filter data in advance:

“NSA routinely sends ISNU [the Israeli Sigint National Unit] minimized and unminimized raw collection”

When Israel finds
data about a U.S. citizen
“ISNU must inform NSA
immediately”

Israel is allows to retain
“any files containing
the identities of U.S. persons
… for no more than one year.”

However, Israelis are required
to “destroy upon recognition”
any communication
“either to or from
an official of the US government”

Senior NSA official in 2008:

“On the one hand,
the Israelis are extraordinarily good
Sigint partners for us,
but on the other,
they target us
to learn our positions
on Middle East problems ...
A [National Intelligence Estimate]
ranked them as
the third most aggressive
intelligence service against the US.”

Want to know the whole story?

Al Jazeera America

“Timeline of
Edward Snowden’s revelations”

http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

Want to help?

Wikileaks · 2,299,332 like this
August 17 at 3:55pm ·

WikiLeaks releases encrypted versions of upcoming publication data ("insurance") from time to time to nullify attempts at prior restraint.

Please mirror:
WikiLeaks insurance 20130815-A: 3.6Gb http://wlstorage.net/torrent/wlinsurance-20130815-A.aes256.torrent
B: 49Gb http://wlstorage.net/torrent/wlinsurance-20130815-B.aes256.torrent
C: 349GB http://wlstorage.net/torrent/wlinsurance-20130815-C.aes256.torrent

We the People

We the People

of the United States, in order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Article. I

Section. 1. All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section. 2. The House of Representatives shall be composed of Members chosen every second Year by the People of the several States, and the Electors in each State shall have the Qualifications requisite for Electors of the most numerous Branch of the State Legislature.

No Person shall be a Representative who shall not have attained to the Age of twenty five Years, and been seven Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State in which he shall be chosen.

Representatives and direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a Term of Years, and excluding Indians not taxed, three fifths of all other Persons. The actual Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct. The Number of Representatives shall not exceed one for every thirty Thousand, but each State shall have at least one Representative; and until such enumeration shall be made, the State of New Hampshire shall be entitled to chuse three, Massachusetts eight, Rhode Island and Providence Plantations one, Connecticut five, New York six, New Jersey four, Pennsylvania eight, Delaware one, Maryland six, Virginia ten, North Carolina five, South Carolina five, and Georgia three.

When vacancies happen in the Representation from any State, the Executive Authority thereof shall issue Writs of Election to fill such Vacancies.

The House of Representatives shall chuse their Speaker and other Officers; and shall have the sole Power of Impeachment.

Section. 3. The Senate of the United States shall be composed of two Senators from each State, chosen by the Legislature thereof, for six Years; and each Senator shall have one Vote.

Immediately after they shall be assembled in Consequence of the first Election, they shall be divided as equally as may be into three Classes. The Seats of the Senators of the first Class shall be vacated at the Expiration of the second Year, of the second Class at the Expiration of the fourth Year, and of the third Class at the Expiration of the sixth Year, so that one third may be chosen every second Year; and if Vacancies happen by Resignation, or otherwise, during the Recess of the Legislature of any State, the Executive thereof may make temporary Appointments until the next Meeting of the Legislature, which shall then fill such Vacancies.

No Person shall be a Senator who shall not have attained to the Age of thirty Years, and been nine Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State for which he shall be chosen.

The Vice President of the United States shall be President of the Senate, but shall have no Vote, unless they be equally divided.

The Senate shall chuse their other Officers, and also a President pro tempore, in the Absence of the Vice President, or when he shall exercise the Office of President of the United States.

The Senate shall have the sole Power to try all Impeachments. When sitting for that Purpose, they shall be on Oath or Affirmation. When the President of the United States is tried, the Chief Justice shall preside: And no Person shall be convicted without the Concurrence of two thirds of the Members present.

Judgment in Cases of Impeachment shall not extend further than to removal from Office, and disqualification to hold and enjoy any Office of honor, Trust or Profit under the United States: but the Party convicted shall nevertheless be liable and subject to Indictment, Trial, Judgment and Punishment, according to Law.

Section. 4. The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators.

The Congress shall assemble at least once in every Year, and such Meeting shall be on the first Monday in December, unless they shall by Law appoint a different Day.

Section. 5. Each House shall be the Judge of the Elections, Returns and Qualifications of its own Members, and a Majority of each shall constitute a Quorum to do Business; but a smaller Number may adjourn from day to day, and may be authorized to compel the Attendance of absent Members, in such Manner, and under such Penalties as each House may provide.

Each House may determine the Rules of its Proceedings, punish its Members for disorderly Behaviour, and, with the Concurrence of two thirds, expel a Member.

Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those Present, be entered on the Journal.

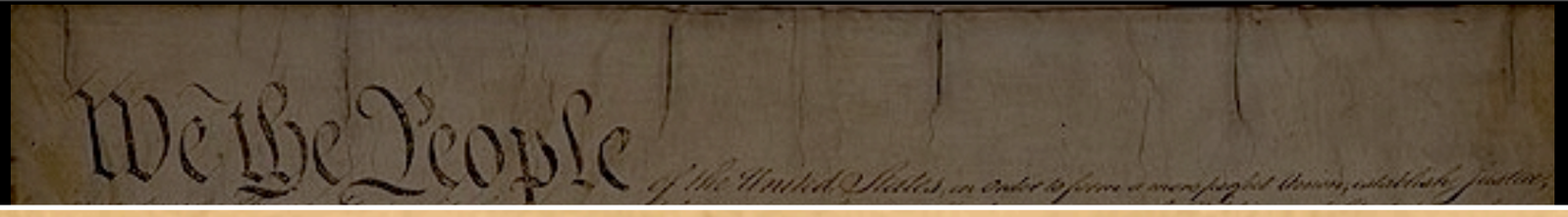
Neither House, during the Session of Congress, shall, without the Consent of the other, adjourn for more than three days, nor to any other Place than that in which the two Houses shall be sitting.

Section. 6. The Senators and Representatives shall receive a Compensation for their Services, to be ascertained by Law, and paid out of the Treasury of the United States. They shall in all Cases, except Treason, Felony and Breach of the Peace, be privileged from Arrest during the Attendance at the Session of their respective Houses, and in going to and returning from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.

No Senator or Representative shall, during the Time for which he was elected, be appointed to any civil Office under the Authority of the United States, which shall have been created, or the Emoluments whereof shall have been encreased during such time; and no Person holding any Office under the United States, shall be a Member of either House during his Continuance in Office.

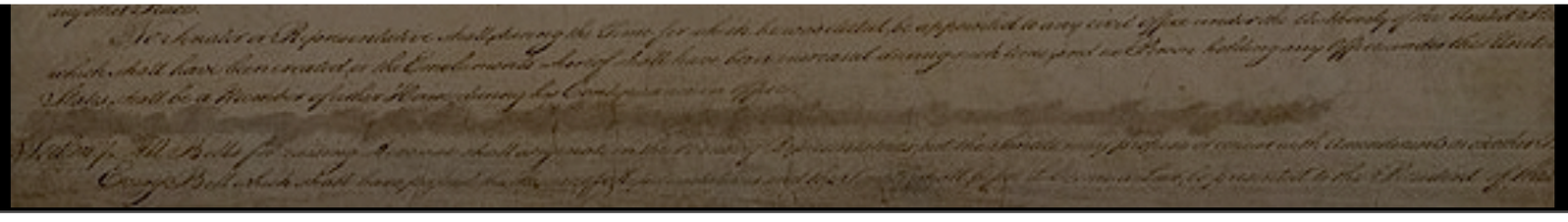
Section. 7. All Bills for raising Revenue shall originate in the House of Representatives; but the Senate may propose or concur with Amendments as on other Bills.

Every Bill which shall have passed the House of Representatives and the Senate, shall, before it become a Law, be presented to the President of the



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.



Exceptions to warrant requirement

✓ Consent

✓ Plain view

✓ Incident to a lawful arrest

✓ Exigent circumstances

✓ Places that merit
low levels of protection
(open fields, cars, borders, &tc.)

Charles I, 1625-1649

American Colonies

James Otis:

“A man’s home is his castle.”

Then

Now

Law
is like
CONCRETE

Olmstead v US (1928)

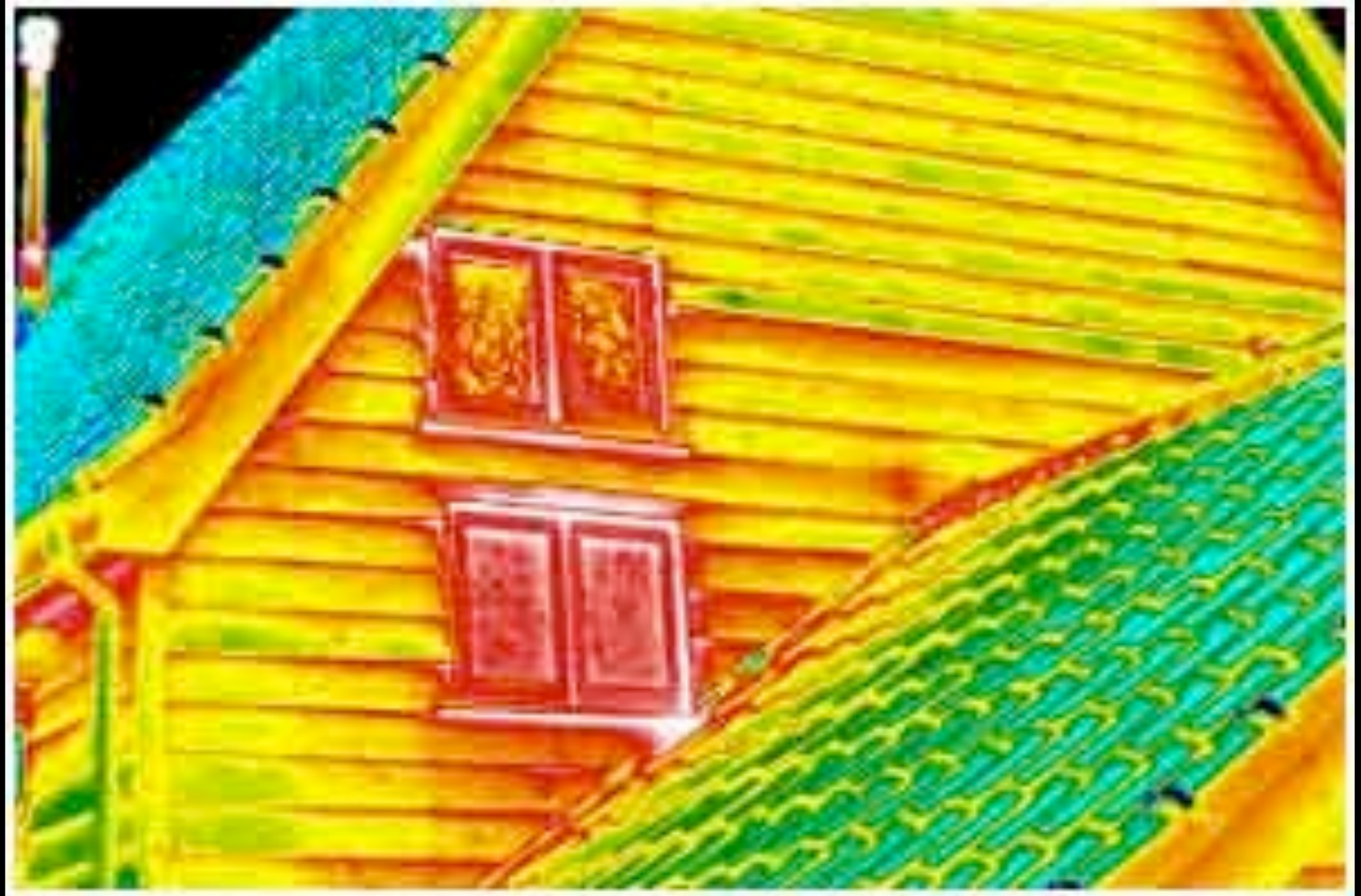
Property of Museum of History & Industry, Seattle

Olmstead v US (1928)

US v Katz (1967)

Kyllo v US (2001)

Kyllo v US (2001)



Kyllo v US (2001)

U.S. v Jones (2012)

U.S. v Jones (2012)

Civil Liberties & Crisis

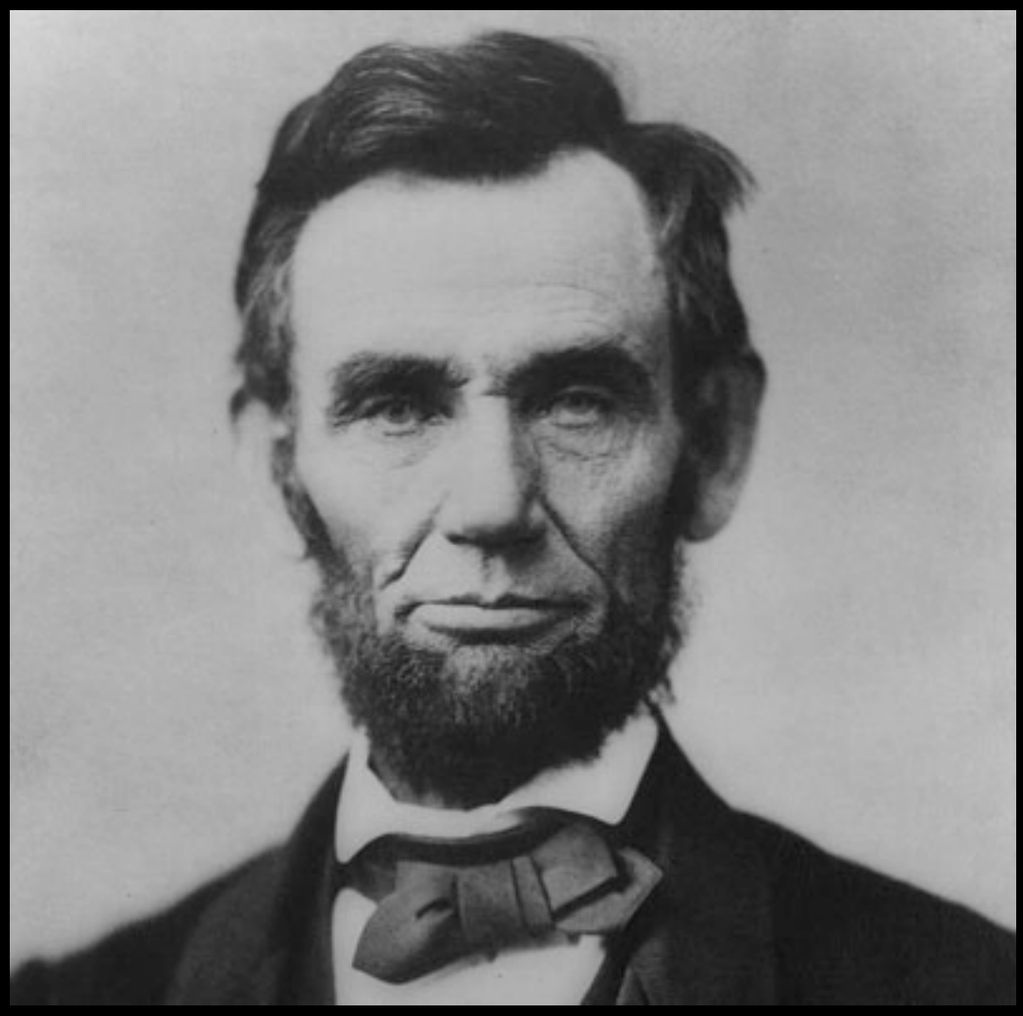
Cicero:

Inter arma enim silent leges

(In times of war, the law falls silent)

1861

President Lincoln suspends Habeas Corpus



World War I

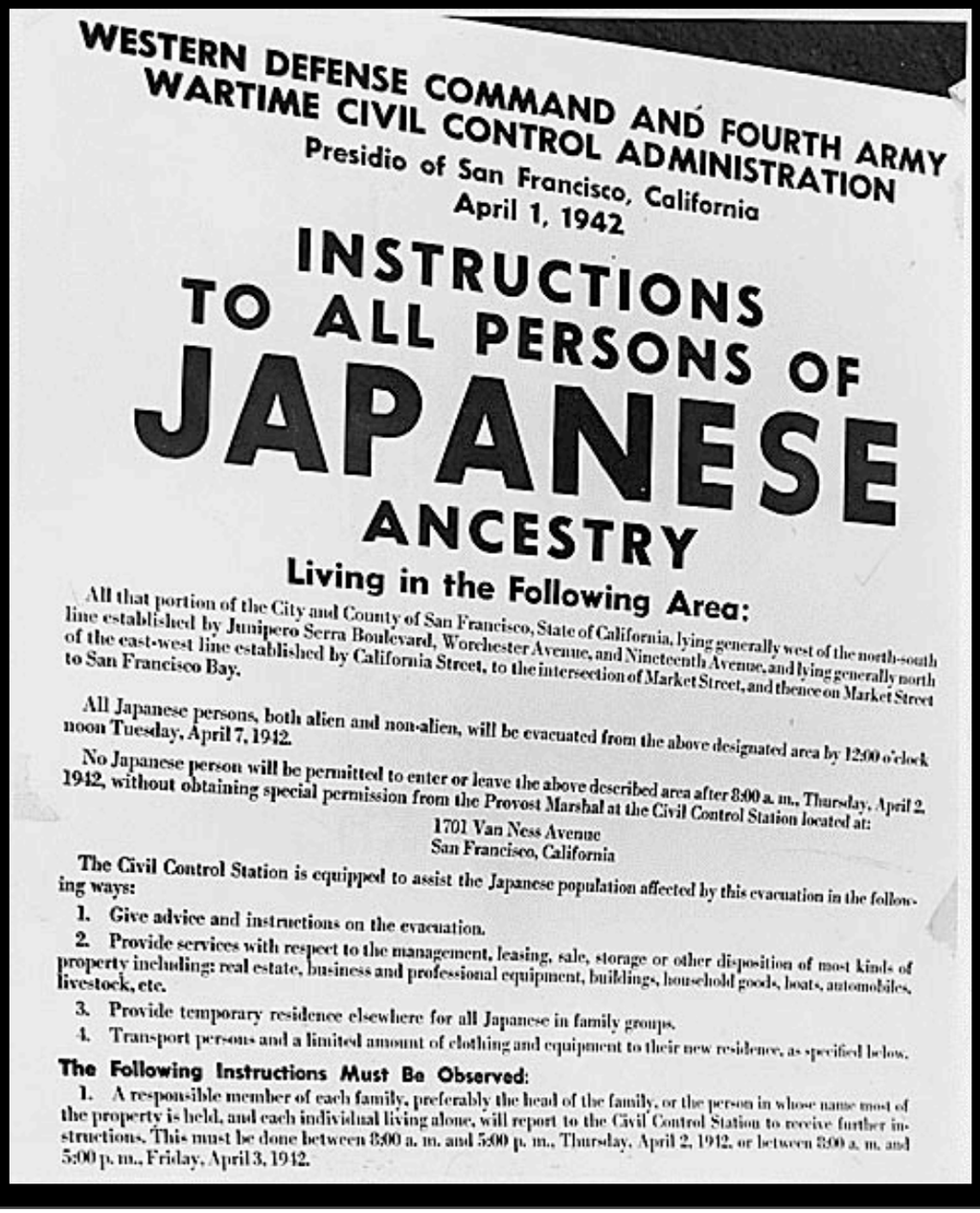
Espionage Act

Restrictions on German & Russian immigrants

WWII

Internment of Japanese Americans

Military Tribunals



WESTERN DEFENSE COMMAND AND FOURTH ARMY
WARTIME CIVIL CONTROL ADMINISTRATION
Presidio of San Francisco, California
April 1, 1942

INSTRUCTIONS
TO ALL PERSONS OF
JAPANESE
ANCESTRY

Living in the Following Area:

All that portion of the City and County of San Francisco, State of California, lying generally west of the north-south line established by Junipero Serra Boulevard, Worchester Avenue, and Nineteenth Avenue, and lying generally north of the east-west line established by California Street, to the intersection of Market Street, and thence on Market Street to San Francisco Bay.

All Japanese persons, both alien and non-alien, will be evacuated from the above designated area by 12:00 o'clock noon Tuesday, April 7, 1942.

No Japanese person will be permitted to enter or leave the above described area after 8:00 a. m., Thursday, April 2, 1942, without obtaining special permission from the Provost Marshal at the Civil Control Station located at:

1701 Van Ness Avenue
San Francisco, California

The Civil Control Station is equipped to assist the Japanese population affected by this evacuation in the following ways:

1. Give advice and instructions on the evacuation.
2. Provide services with respect to the management, leasing, sale, storage or other disposition of most kinds of property including: real estate, business and professional equipment, buildings, household goods, boats, automobiles, livestock, etc.
3. Provide temporary residence elsewhere for all Japanese in family groups.
4. Transport persons and a limited amount of clothing and equipment to their new residence, as specified below.

The Following Instructions Must Be Observed:

1. A responsible member of each family, preferably the head of the family, or the person in whose name most of the property is held, and each individual living alone, will report to the Civil Control Station to receive further instructions. This must be done between 8:00 a. m. and 5:00 p. m., Thursday, April 2, 1942, or between 8:00 a. m. and 5:00 p. m., Friday, April 3, 1942.

Cold War

Surveillance & investigation of political groups

House Un-American Activities Committee

Vietnam War
& Civil Rights Movements

Targeting of protesters

Expansion of FBI powers

9/11

How is
9/11
different?

Technology…

✓ changes how threats operate

✓ changes how governments respond

Nature of threats different

✓ Non-state-sponsored

✓ Less hierarchical

✓ Dispersed

✓ Anonymous

Our response is different:

Ubiquitous surveillance

US Government's Response

PATRIOT Act § 215

FISA Title VII § 702

National Security Letters

2001

An Act

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001".

2001

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

Allows government to get
"any tangible things ... relevant to a ...
national security investigation ...
to protect against
international terrorism
or clandestine intelligence activities"

Expands *types* of records

Before

Only:

✓ Hotel & motel records

✓ Car & truck rentals

✓ Storage rentals

→

Now

“Any tangible things”

Easier to get FISA warrant

Before		Now
FBI had to show "specific articulable facts" that the subject was a "foreign power or the agent of a foreign power"	→	Things are sought for a foreign intelligence investigation

Expanded government access
without probable cause of a crime

✓ Business documents
✓ 3rd party documents
✓ Electronic communications

FBI given greater latitude
to go on “fishing expeditions”

PLEASE BE AWARE that under Section 215 of the USA PATRIOT ACT agents of the Federal Government are empowered to monitor your use of the Internet and to have access to knowing what library books and other materials you use and check out; be aware also that Librarians are prohibited upon of prosecution from letting you know that the Government is investigating your reading habits and computer use. The Library and its staff will do whatever is possible to protect your privacy.

1978 / Amended in 2008

Public Law 95-511
95th Congress

An Act

To authorize electronic surveillance to obtain foreign intelligence information.

Oct. 25, 1978
[S. 1566]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

Foreign Intelligence Surveillance Act of 1978.
50 USC 1801 note.

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

1978 / Amended in 2008

An Act

To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008" or the "FISA Amendments Act of 2008".

1978 / Amended in 2008

"SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

"(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Allows government to collect electronic communications

Targets must be foreign

Must relate to national security ~~threat~~

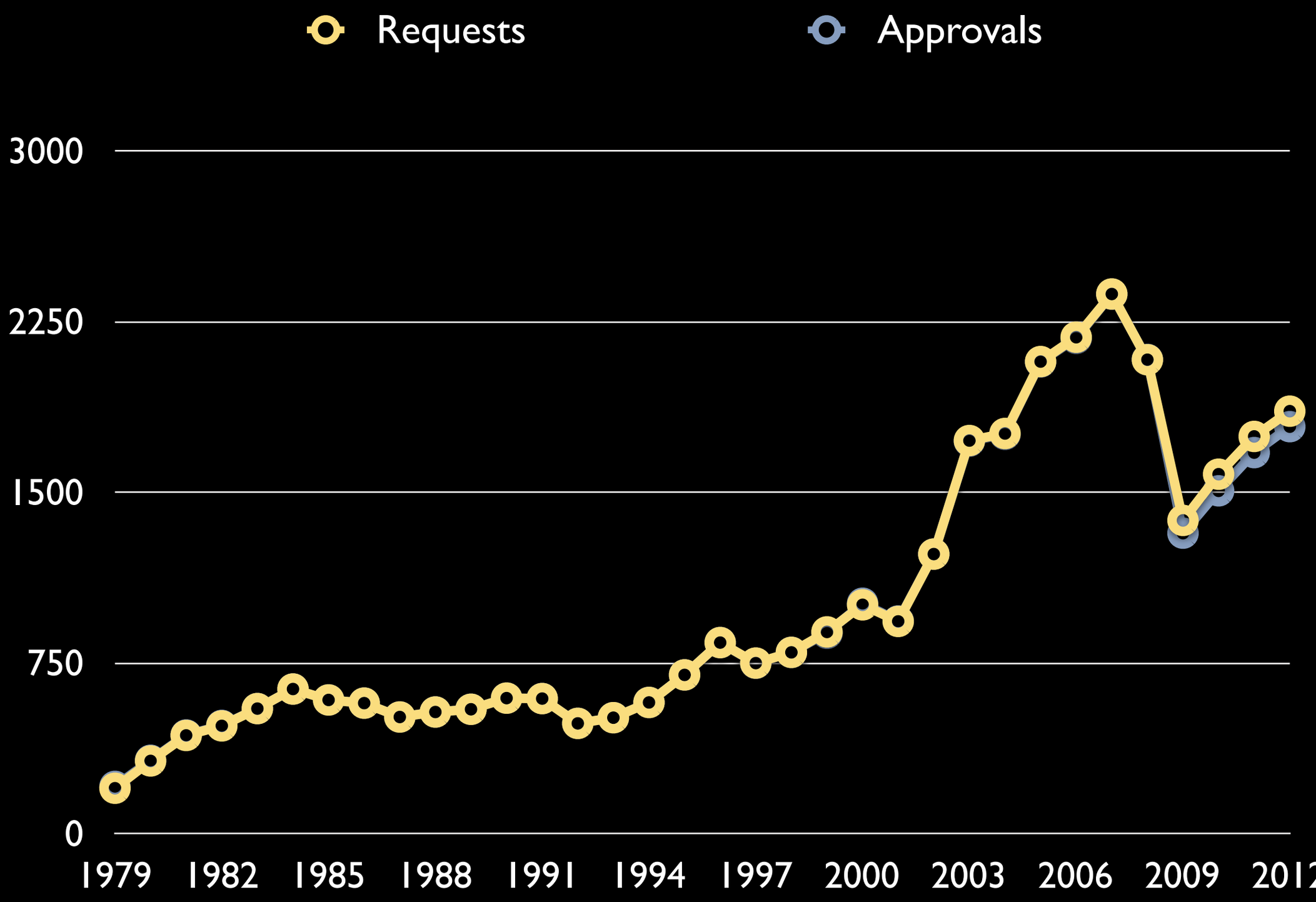
FISA Court

Appointed by SCOTUS Chief Justice

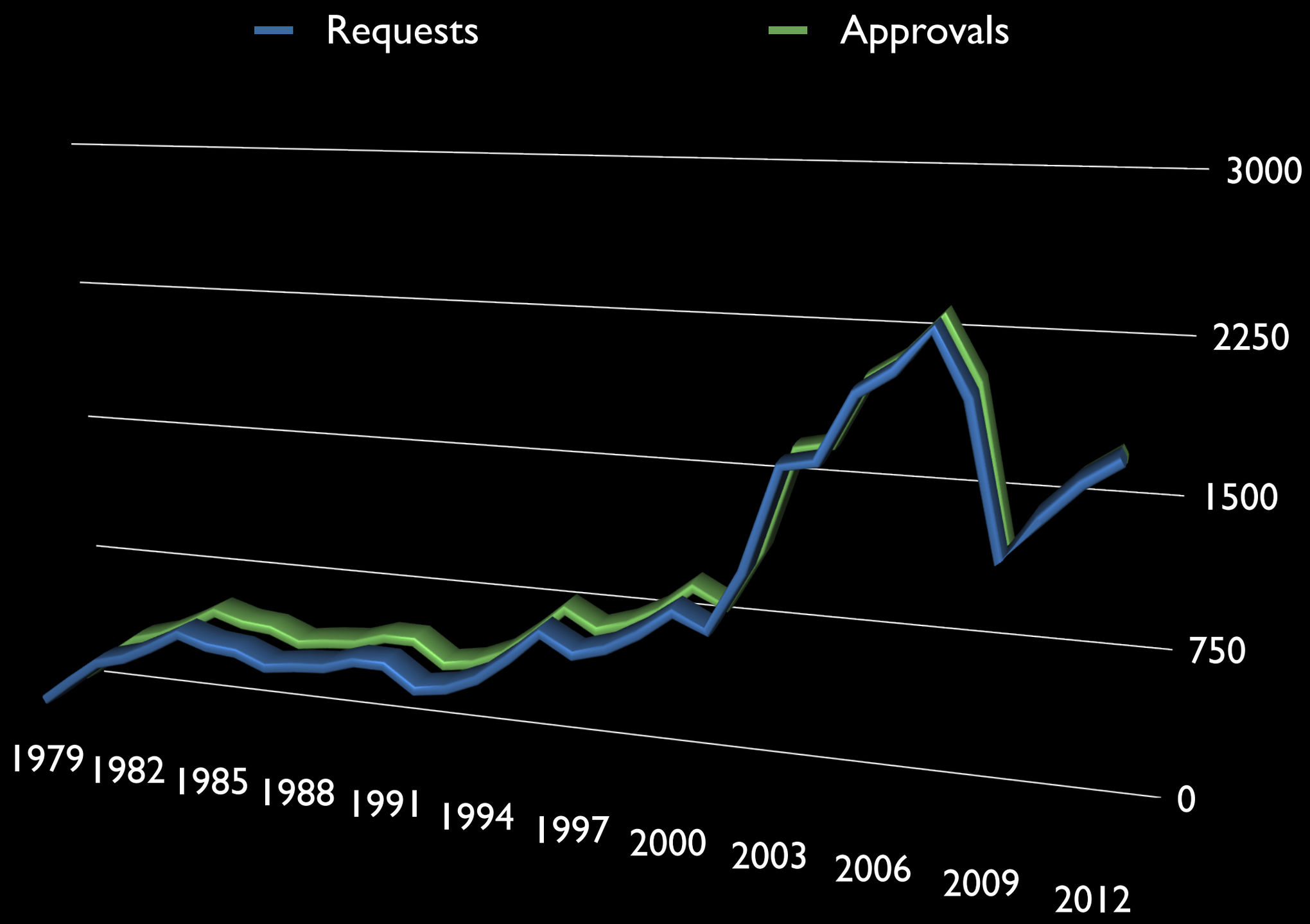
Meets in secret

Oversees application of FISA

Foreign Intelligence Surveillance Act



Foreign Intelligence Surveillance Act



1978
Amended in 1986, 1993, 2001, 2006

National Security Letters

Can request only
non-content information, e.g.:

✓ Store purchases
✓ Bank deposits & withdrawals
✓ Phone numbers dialed
✓ Website visits & searches
✓ Sender/recipient email addresses

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. NH-43906

New Haven Division
600 State Street
New Haven, Connecticut 06511

May 19, 2005

Mr. Kenneth Sutton
Systems and Telecommunication Manager
Library Connection, Inc.
599 Matianuck Avenue
Windsor, Connecticut

Dear Mr. Sutton:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) any and all subscriber information, billing information and access logs of any person or entity related to the following:

IP Address: 216.47.180.118, Date: 02/15/2005; Time: 16:00 to 16:45 (PM) EST

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the New Haven field office of the FBI. Electronic versions of the records are requested, if available. Any questions you have regarding this request should be directed only to the New Haven field office. Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation or electronic communication.

Non-expiring gag order

Independent of legal courts

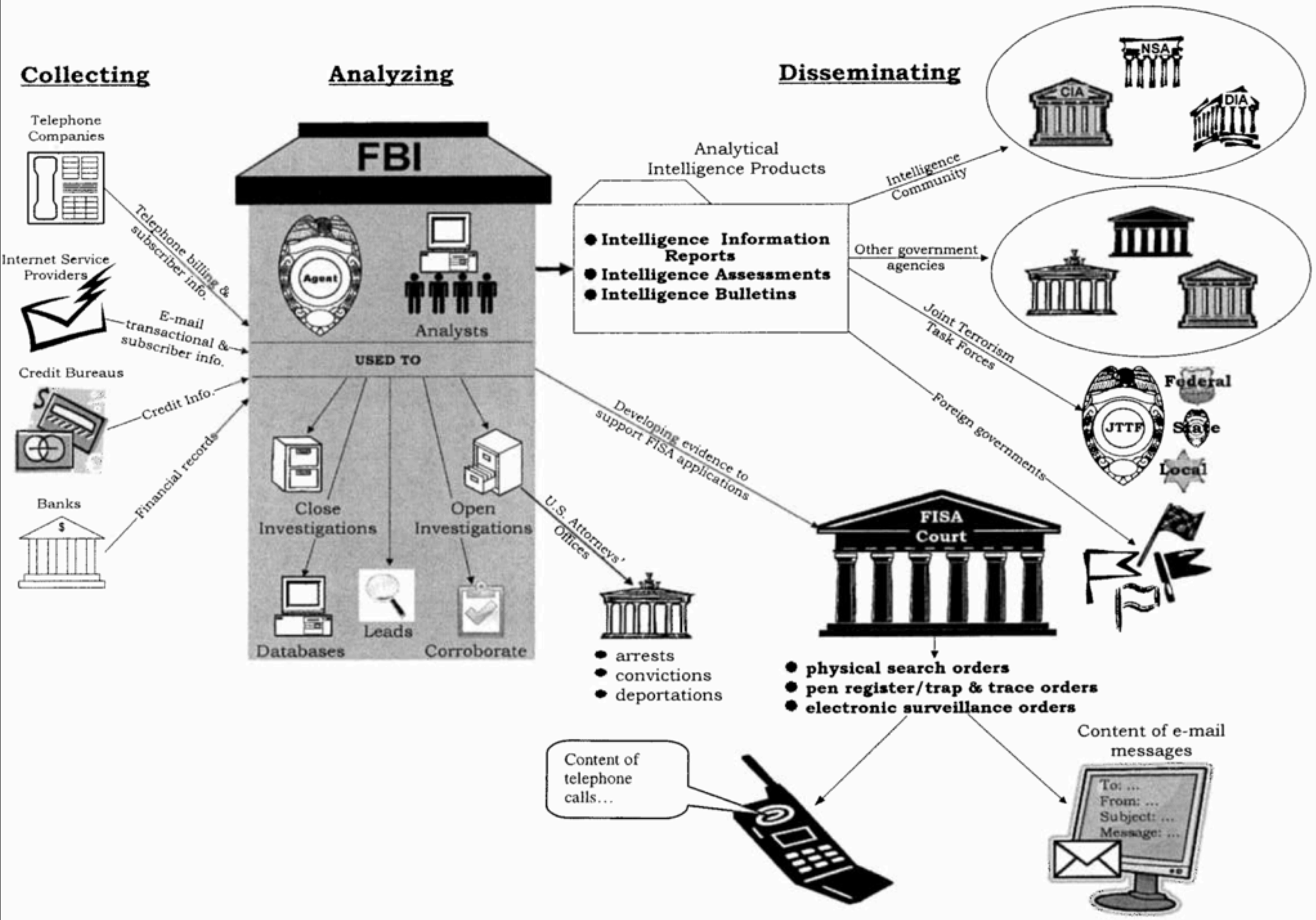
Not a subpoena

Used by

✓ FBI
✓ CIA
✓ Pentagon

2003–2006
FBI issued 192,499 NSL requests

How the FBI Uses National Security Letters



There are some tradeoffs involved … It's important to recognize that you can't have 100% security, and also then have 100% privacy, and zero inconvenience. We're going to have to make some choices as a society.

It is neither desirable
nor is it remotely likely
that civil liberty will occupy
as favored a position in wartime
as it does in peacetime.
The laws will thus
not be silent in time of war,
but they will speak
with a somewhat different voice.

William Rehnquist,
Former Supreme Court
Chief Justice

The solution: encryption

Who’s the threat?

The guy in the coffee shop?

Corporations?

The government?

Thieves & Snoops

The Goal:

Prevent the snoop
from reading your stuff

Not worried about
corporations & the government

Email over HTTPS

✓ Gmail

✓ ~~Hotmail~~ Outlook.com

✓ Yahoo Mail*

* HTTPS not on by default

IM

✓ Skype

✓ Google ~~Chat~~ Hangouts

✓ Pidgin or Adium with OTR
(Off the Record)

Extensions

✓ HTTPS Everywhere

✓ Force-TLS

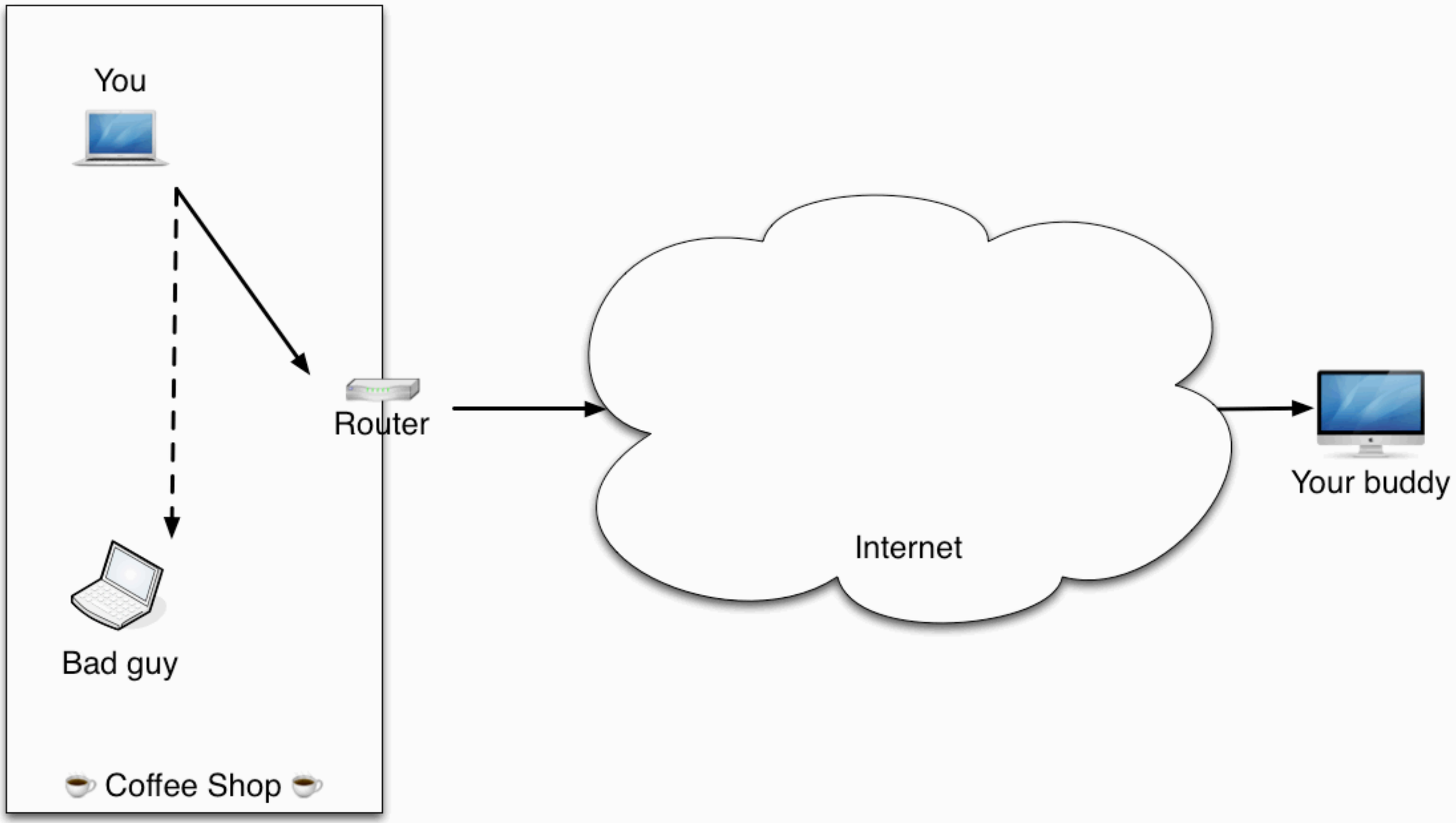
Extensions

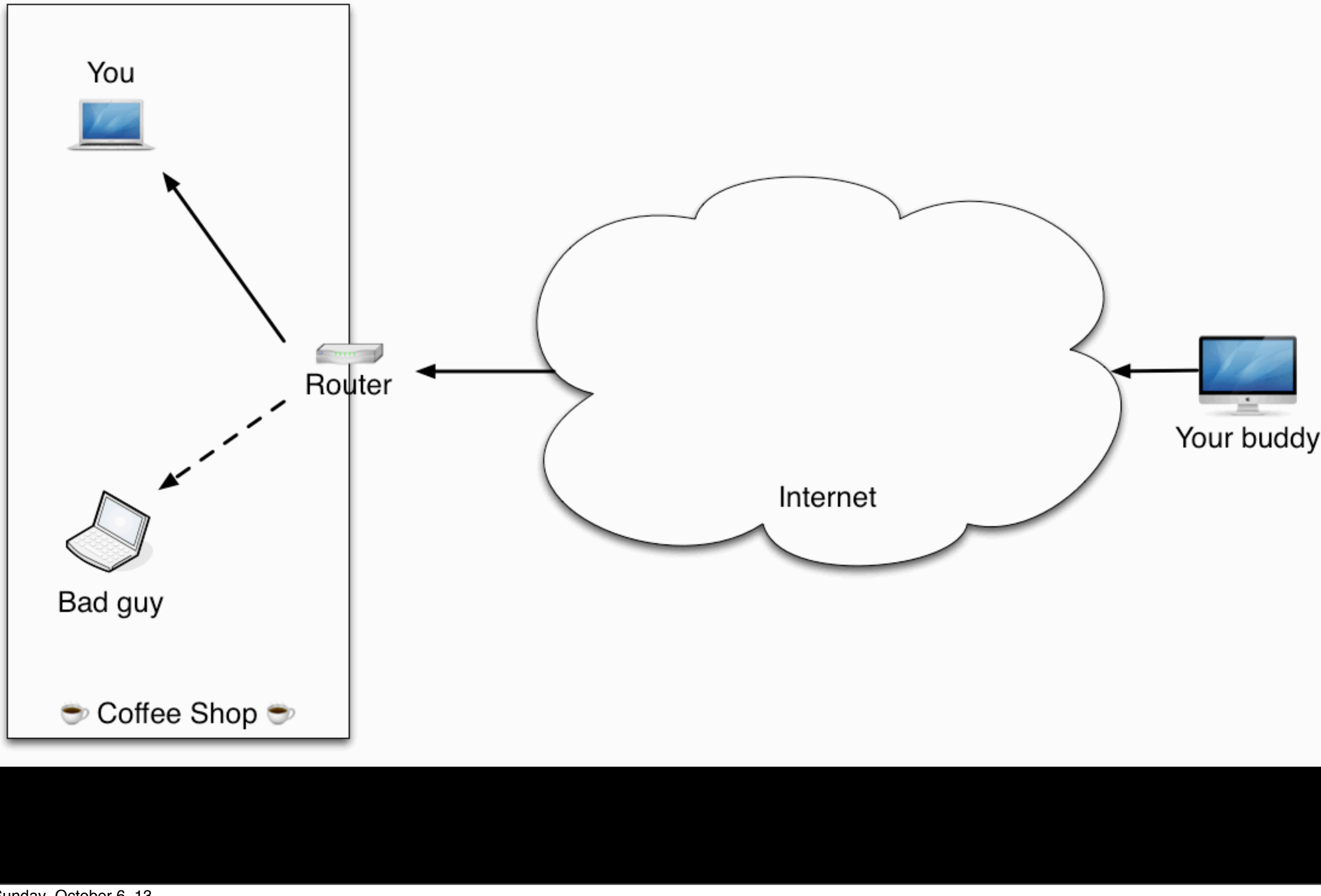
✓ Secure Login Helper

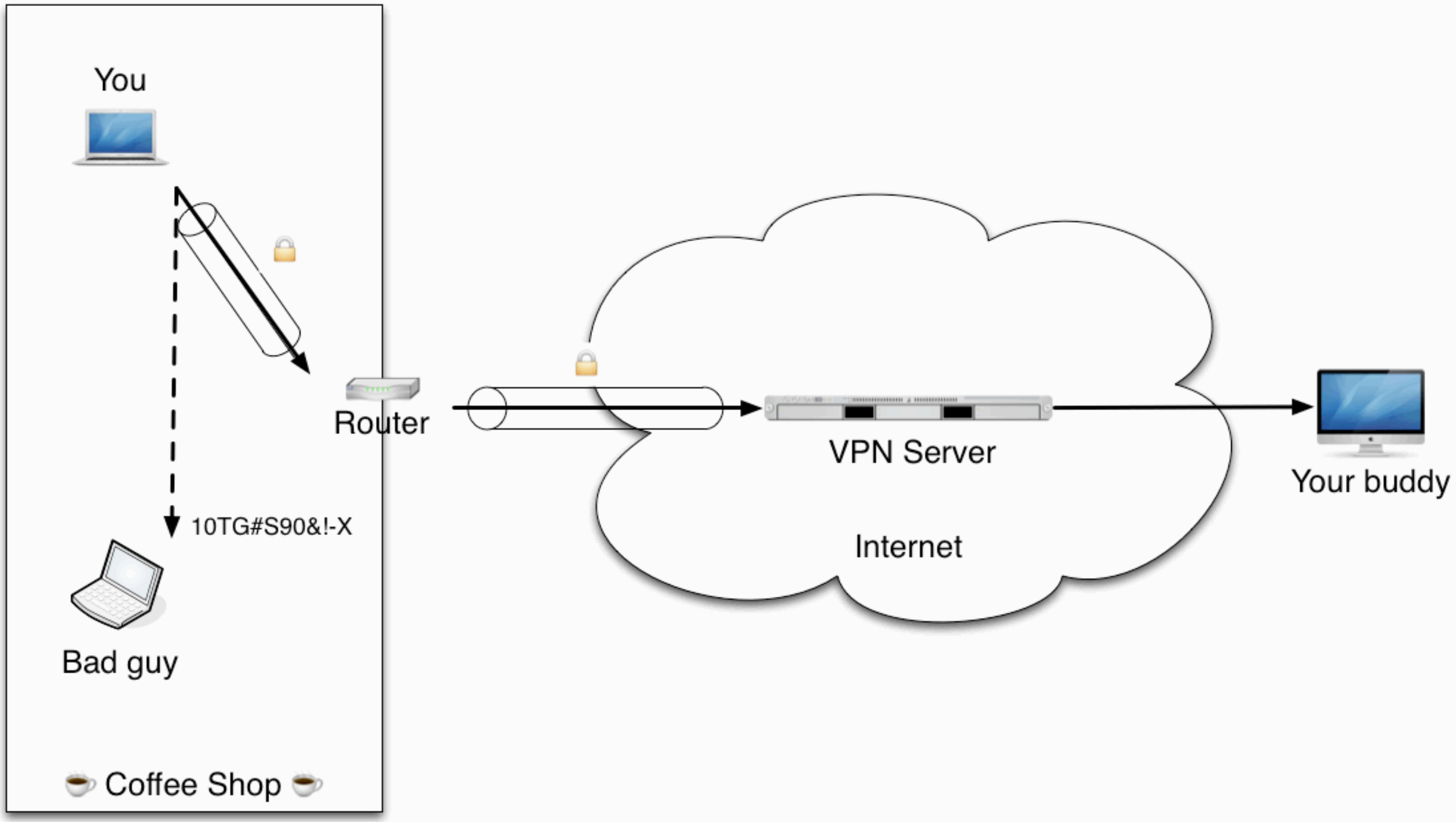
✓ KB SSL Enforcer

VPN
(*Virtual Private Network*)
encrypts all Internet traffic
in an encrypted tunnel
between you & the VPN server

After that,
it’s not in the encrypted tunnel


You
Router
Internet
Your buddy
Bad guy
Coffee Shop


You
Router
Bad guy
Coffee Shop
Internet
Your buddy


You
10TG#S90&!-X
Bad guy
Coffee Shop
Router
VPN Server
Internet
Your buddy

StrongVPN
www.strongvpn.com
$7/month

VPNtunnel
www.vpntunnel.com
5€/month

WhatIs MyIPAddress .com

My IP | IP Lookup | Blacklist Check | Trace Email | Speed Test | Hide IP | Change IP | IP Tools | FAQs | Forums | Search

What Is My IP Address? (Now detects many proxy servers)

Location not accurate? Update your IP location

IP Information: 5.254.129.67

ISP: Netalia AB
Organization: Portlane Networks AB
Connection: Broadband
Services: None Detected
Country: Sweden

Don't want this ↑↑↑ known? Hide your IP details

5.254.129.67 Additional IP Details

WhatIs MyIPAddress .com

My IP | IP Lookup | Blacklist Check | Trace Email | Speed Test | Hide IP | Change IP | IP Tools | FAQs | Forums | Search

What Is My IP Address? (Now detects many proxy servers)

Location not accurate? Update your IP location

IP Information: 5.254.129.67

ISP: Netalia AB
Organization: Portlane Networks AB
Connection: Broadband
Services: None Detected
Country: Sweden

Don't want this ↑↑↑ known? Hide your IP details

5.254.129.67 Additional IP Details

No logging!

Corporations

The Goal:

Stop getting tracked
by corporations

Not a defense
against snoops or the government

If you’re not paying for a service,
you’re the product,
not the customer

Don’t give your data away

Minimize tracking

Google™

Google
TM

Duck Duck Go

www.duckduckgo.com

Search DuckDuckGo

https://duckduckgo.com

Apps | S-Foc | Ent | RSG | G | WS | Soc | Apps | lets | News | Save | Other Bookmarks

DuckDuckGo

Search anonymously. Find instantly.

Press | Help spread better search. | Add to Browser | Set as Homepage | More

missouri scholars academy

https://duckduckgo.com/?q=missouri+scholars+academy

Apps | S-Foc | Ent | RSG | G | WS | Soc | Apps | lets | News | Save | Other Bookmarks

missouri scholars academy

More

Missouri Scholars Academy

Missouri Scholars Academy, or MSA, is a three-week residential summer program held on the University of Missouri campus in Columbia, Missouri for 330 of Missouri's top rising high school juniors.

More at Wikipedia

Education in Missouri

University of Missouri

Add to Browser

Give feedback

Try this search on:

Wikipedia
Facebook
CollegeConfidential ...
Vimeo
Flickr
LinkedIn
Urban Dictionary

Manage Hiding

Missouri Scholars Academy block

A three-week academic program for 330 of Missouri's gifted students who are ready to begin their junior year in high school. The **academy** is a residential program held on the campus of the University of Missouri-Columbia.

moscholars.org More from moscholars.org ▸

Missouri Scholars Academy - Camp | Precollege | University of ... block

Sunday, June 09, 2013 - Saturday, June 29, 2013 The **Missouri Scholars Academy** is a three-week academic program for 330 of Missouri's gifted students who are ready to begin their junior year in high school.

musis1.missouri.edu/precollege/camp.cfm?camp=Missouri Schol... More from musis1.missouri.edu ▸

[PDF] Missouri Scholars Academy block

Missouri Scholars Academy. What It Is. The **Missouri Scholars Academy** is a three-week, residential summer program held on the Columbia campus of the University of Missouri.

dese.mo.gov/divimprove/gifted/documents/mo_scholars... More from dese.mo.gov ▸

Missouri Scholars Academy | Facebook block

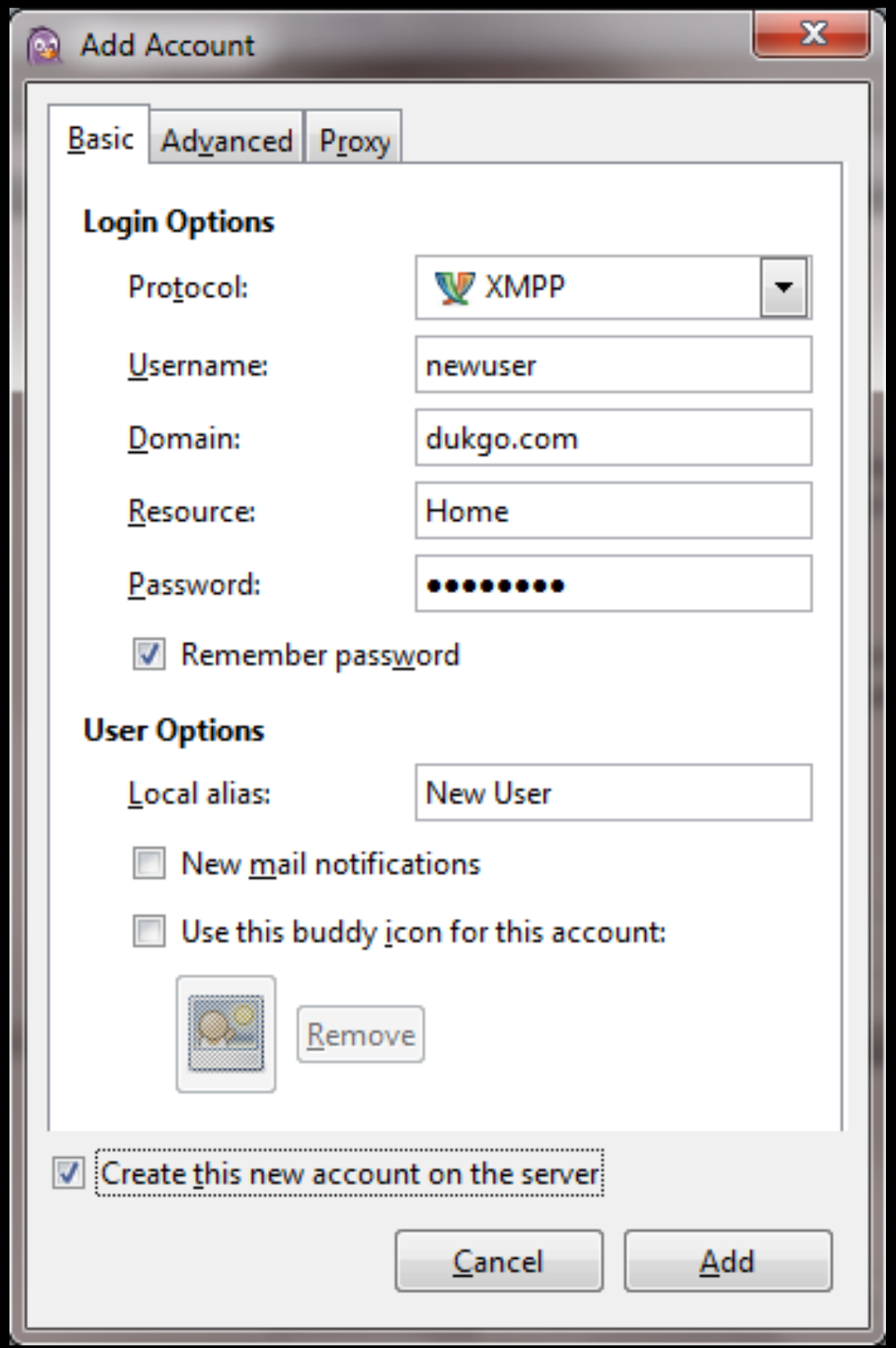
Missouri Scholars Academy. 265 likes · 9 talking about this.

facebook.com/MissouriScholarsAcademy More from facebook.com ▸

Missouri Scholars Academy - College Confidential block

Does anyone know the cutoff PSAT and PLAN scores for the **Missouri Scholars Academy** thing this year?

“We don’t send your searches
to other sites.
Or store
any personal information at all.”



DuckDuckGo XMPP/Jabber service

http://chnsa.ws/ee

Ghostery

www.ghostery.com

1,300+ companies in its database

2,800+ individual tracking elements

✓ Advertiser
✓ Analytics
✓ Beacon
✓ Widget
✓ Privacy

Rank	Name	Type	Rank Change	Count
1	Google Analytics	AN	=	112
2	Google Adsense	AD	=	39.5
3	Facebook Connect	W	=	35
4	Facebook Social Plugins	W	=	32.2
5	Google +1	W	=	31.1
6	ScoreCard Research Beacon	B	=	25.4
7	DoubleClick	AD	=	23
8	Twitter Button	W	=	19.9
9	Quantcast	AD	=	17.3
10	AddThis	W	=	16.8
11	Omniture (Adobe Analytics)	B	=	10.2
12	OpenX	AD	=	9.3
13	Google AdWords Conversion	AD	=	8
14	Amazon Associates	AD	↑	7.1
15	ShareThis	W	↓	7

AdBrite
Adroit Digital Solutions
Advertising.com
AMP Platform
AppNexus
Audience Science
BlueKai
Brilig
ChartBeat
ChoiceStream
Dataium
DoubleClick
DoubleClick Bid Manager
Drawbridge
Evidon Notice
eXelate
Facebook Connect
Facebook Exchange (FBX)
Facebook Social Plugins
Gigya Socialize
Google +1
Google Adsense
Google Analytics
i-Behavior
Intent Media
Krux Digital
LinkedIn Widgets
Lotame
Media Innovation Group
MediaMind
MSN Ads
NextAction
Omniture
RapLeaf
Right Media
Rocket Fuel
ScoreCard Research Beacon
Tapad
TargusInfo
TradeDesk
Turn
Twitter Button
Typekit by Adobe
VigLink

24/7 Media
[x+1]
Adap.tv
AdBrite
AdMeld
Adometry
AdSafe
ADTECH
Advertising.com
Aggregate Knowledge
AMP Platform
AppNexus
Audience Science
Bizo
BlueKai
BrightRoll
Brilig
ChoiceStream
ContextWeb
CoreAudience
Criteo
DataXu
Datran
Digilant
DoubleClick
Drawbridge
Evidon Notice
eXelate
Google Adsense
Google AdWords Conversion
Google Analytics
i-Behavior
Intent Media
Invite Media
LeadBack
Lotame
Media Innovation Group
Media6Degrees
MediaMath
NetRatings SiteCensus
NextAction
nPario
OpenX
PubMatic
Quantcast
Quantcast Notice
RapLeaf
Resonate Networks
Right Media
Rocket Fuel
Rubicon
ScoreCard Research Beacon
Tacoda
Tapad
TargusInfo
TidalTV
TradeDesk

ghostery worst web | KnowYourElements | The Purple Box | Th | Suns up. Time for b | Thank you Ghostery | PCWorld – News, tip | DoubleClick — Anal

www.pcworld.com

Apps | S-Foc | Ent | RSG | G | WS | Soc | Apps | lets | News | Save | Other Bookmarks

ChartBeat
DoubleClick
DoubleClick Spotlight
Facebook Connect
Gigya Socialize
Google +1
LinkedIn Widgets
MSN Ads
NetRatings SiteCensus
Omniture (Adobe Analytics)
Pinterest
Reddit
Twitter Button
Typekit by Adobe

PCWorld | Macworld | TechHive | Sign In | Join

E3 2013

Full Coverage on PCWorld

READ MORE

PCWorld

Google's Project Loon wants to spread Net access with high-flying balloons

Facebook, Microsoft disclose FISA requests (sort of)

Both companies asked for and received permission to disclose FISA and other government requests.

NEWS | REVIEWS | HOW-TO | BUSINESS · LAPTOPS · COMPUTERS · PRINTERS · SECURITY · SOFTWARE · WINDOWS · PHONES · VIDEO

Select Text to Edit

Accessibility Options

computers/tablets

ghostery worst website | KnowYourElements.com | The Purple Box | The Ho | Suns up. Time for bed or | Thank you Ghostery. Thi | PCWorld – News, tips an

www.pcworld.com

Apps | S-Foc | Ent | RSG | G | WS | Soc | Apps | lets | News | Save | Other Bookmarks

Ghostery found the following:

~~ChartBeat~~ more info
~~http://static.chartbeat.com/js/chartbeat.js~~

~~DoubleClick~~ more info
~~http://ad.doubleclick.net/ad/pcw.main.trackingpixel/...~~
~~http://ad.doubleclick.net/ad/pcw.main.trackingpixel/...~~

~~DoubleClick Spotlight~~ more info
~~http://ad.doubleclick.net/activity;dc_pixel_url=idgt.c...~~

~~Facebook Connect~~ more info
~~http://connect.facebook.net/en_US/all.js#xfbml=1&a...~~
~~http://connect.facebook.net/en_GB/all.js~~

~~Gigya Socialize~~ more info
~~http://cdn.gigya.com/js/socialize.js?apiKey=2_eyT43n...~~

Edit Blocking Options

PCWorld | Macworld | TechHive | Sign In

E3 2013

PCWorld

Google's Project Loon wants to spread Net access with high-flying balloons

Facebook, Microsoft disclose FISA requests

Both companies asked for and received permission to disclose FISA and other government requests.

NEWS | REVIEWS | HOW-TO | BUSINESS · LAPTOPS · COMPUTERS · PRINTERS · SECURITY · SOFTWARE · WINDOWS · PHONES · VIDEO

Ghostery – results.png | Ghostery – 70 results.png | Ghostery logo.png | Show All

ghostery worst website | KnowYourElements.com | The Purple Box | The Ho | Suns up. Time for bed or | Thank you Ghostery. Thi | PCWorld – News, tips an

www.pcworld.com

Apps | S-Foc | Ent | RSG | G | WS | Soc | Apps | lets | News | Save | Other Bookmarks

Ghostery found the following:

http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-...

Omniture (Adobe Analytics) more info
http://www.pcworld.com/www.pcw/js/analytics/om...

Pinterest more info
http://assets.pinterest.com/js/pinit.js

Reddit more info
http://www.reddit.com/static/button/button3.js

Twitter Button more info
http://platform.twitter.com/widgets/follow_button.1...
http://platform.twitter.com/widgets/tweet_button.1...

Typekit by Adobe more info
http://p.typekit.net/p.gif?a=620309&f=6037.6038.604...

Edit Blocking Options

PCWorld Macworld TechHive Sign In

E3 2013

PCWorld

Google's Project Loon wants to spread Net access with high-flying balloons

Facebook, Microsoft disclose FISA requests

Both companies asked for and received permission to disclose FISA and other government requests.

NEWS REVIEWS HOW-TO BUSINESS · LAPTOPS · COMPUTERS · PRINTERS · SECURITY · SOFTWARE · WINDOWS · PHONES · VIDEO

Ghostery – results.png | Ghostery – 70 results.png | Ghostery logo.png | Show All

Ghostery Knowledge Page

Like Ghostery? Rate It! Also, Take our Survey!

About DoubleClick:

DoubleClick operates: DoubleClick, DoubleClick DART, DoubleClick Floodlight, DoubleClick Spotlight

doubleclick by Google

In Their Own Words

"Google's DoubleClick products provide ad management and ad serving solutions to companies that buy, create or sell online advertising."

Website: http://www.google.com/doubleclick/

Industry Affiliations:

Learn More

Releases, reviews, and research at Ghostery's Purple Box blog

Follow Ghostery on Twitter

Friend Ghostery on Facebook

Download Ghostery now for free

Need help? Visit our support forums.

DoubleClick was found on over **100000** sites. Here's a sample:

1. www.facebook.com
2. www.youtube.com
3. www.imdb.com
4. www.heise.de
5. www.amazon.com

Privacy Information

Privacy Contact

© 2013 Ghostery, a service of Evidon, Inc. All rights reserved. 10 East 39th Street, 8th Floor, New York, NY 10016

Sunday, October 6, 13

Industry Affiliations:

1. www.facebook.com
2. www.youtube.com
3. www.imdb.com
4. www.heise.de
5. www.amazon.com

Privacy Information

Privacy Policy:

http://www.google.com/intl/en/policies/privacy/

Data Collected:

Anonymous (Ad Views, Analytics, Browser Information, Cookie Data , Date/Time, Demographic Data, Hardware/Software Type, Interaction Data , Page Views , Serving Domains)
Pseudonymous (IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII))
PII (Phone Number)

Data Sharing:

Anonymous data is shared with 3rd parties.

Data Retention:

Undisclosed

Privacy Contact

DoubleClick

111 Eighth Avenue , 10th Floor , New York, NY, 10011
Email: privacydept@doubleclick.com

Privacy contact URL:

http://www.google.com/support/websearch/bin/request.py?form_type=user&stage=fm&user_type=user&contact_type=privacy

© 2013 Ghostery, a service of Evidon, Inc. All rights reserved. 10 East 39th Street, 8th Floor, New York, NY 10016

Sunday, October 6, 13

BROWSER	DETECTION	CONTROL	CURRENT VERSION	DOWNLOAD
Firefox	Full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	2.9.5	Download Ghostery for Firefox now!
Safari	Full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	1.4.2	Download Ghostery for Safari now!
Google Chrome	Full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	4.1.2	✓ Installed
Opera	Almost full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	0.10.0 0.12.0 (Opera Next)	Download Ghostery for Opera now!
Internet Explorer	Full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	3.1.0	Download Ghostery for Internet Explorer now!

MOBILE BROWSER	DETECTION	CONTROL	CURRENT VERSION	DOWNLOAD
iOS Ghostery for Mobile - iOS	Full detection of tracker scripts, img tags, and iframes from over 1000 data collection services	Blocking capability for each detected element	1.2	Get Ghostery from iTunes Store now!

Google's Project Loon wants to spread Net access with high-flying balloons

How to use Facebook

AT&T 11:17 PM 96%

Back

Trackers

- BlueKai
- ChartBeat
- Commission Junction
- DoubleClick
- eXelate
- Facebook Connect
- Facebook Social Plugins
- Gigya Socialize
- Google +1

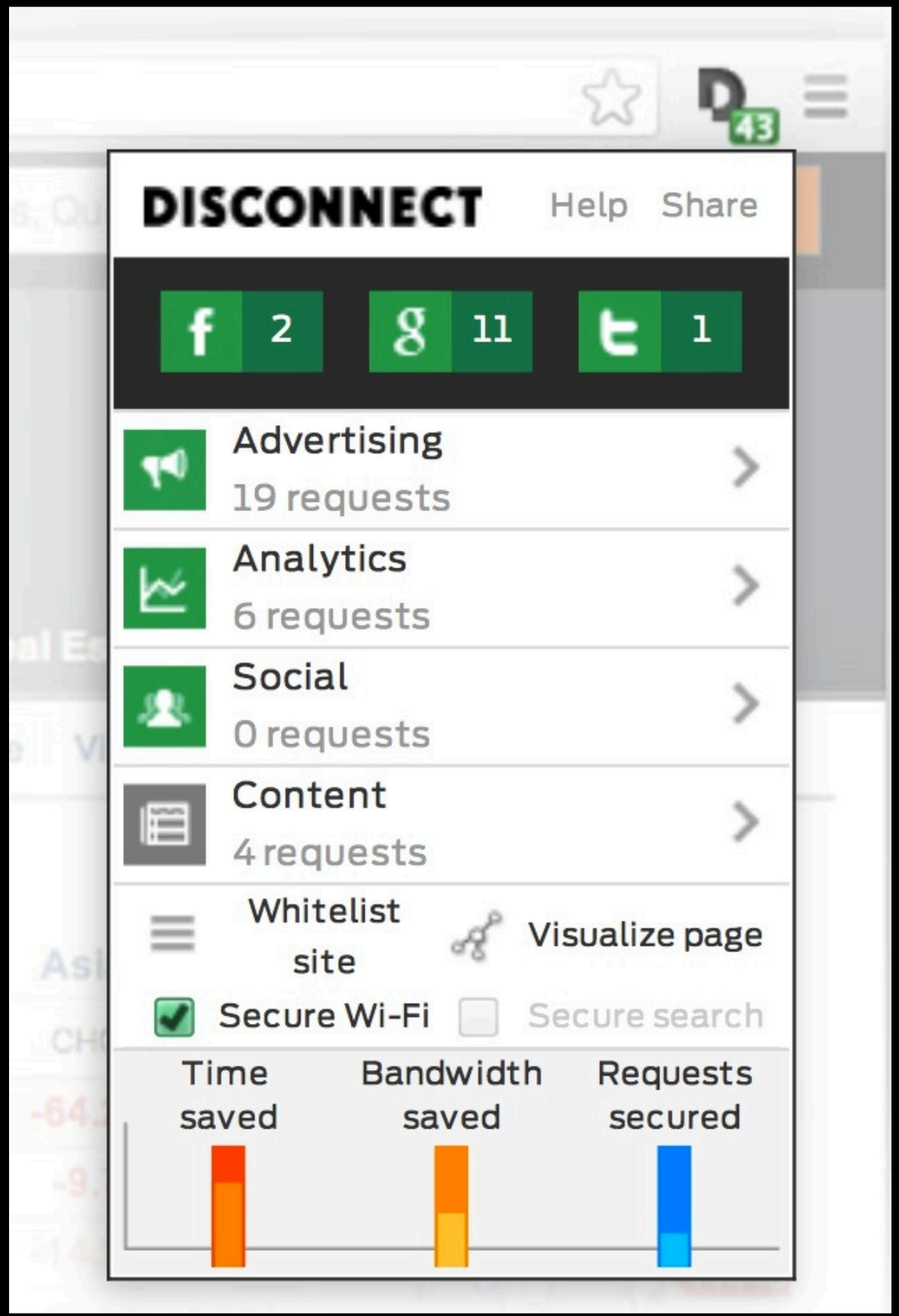
More Info Block

Disconnect

disconnect.me

Open source

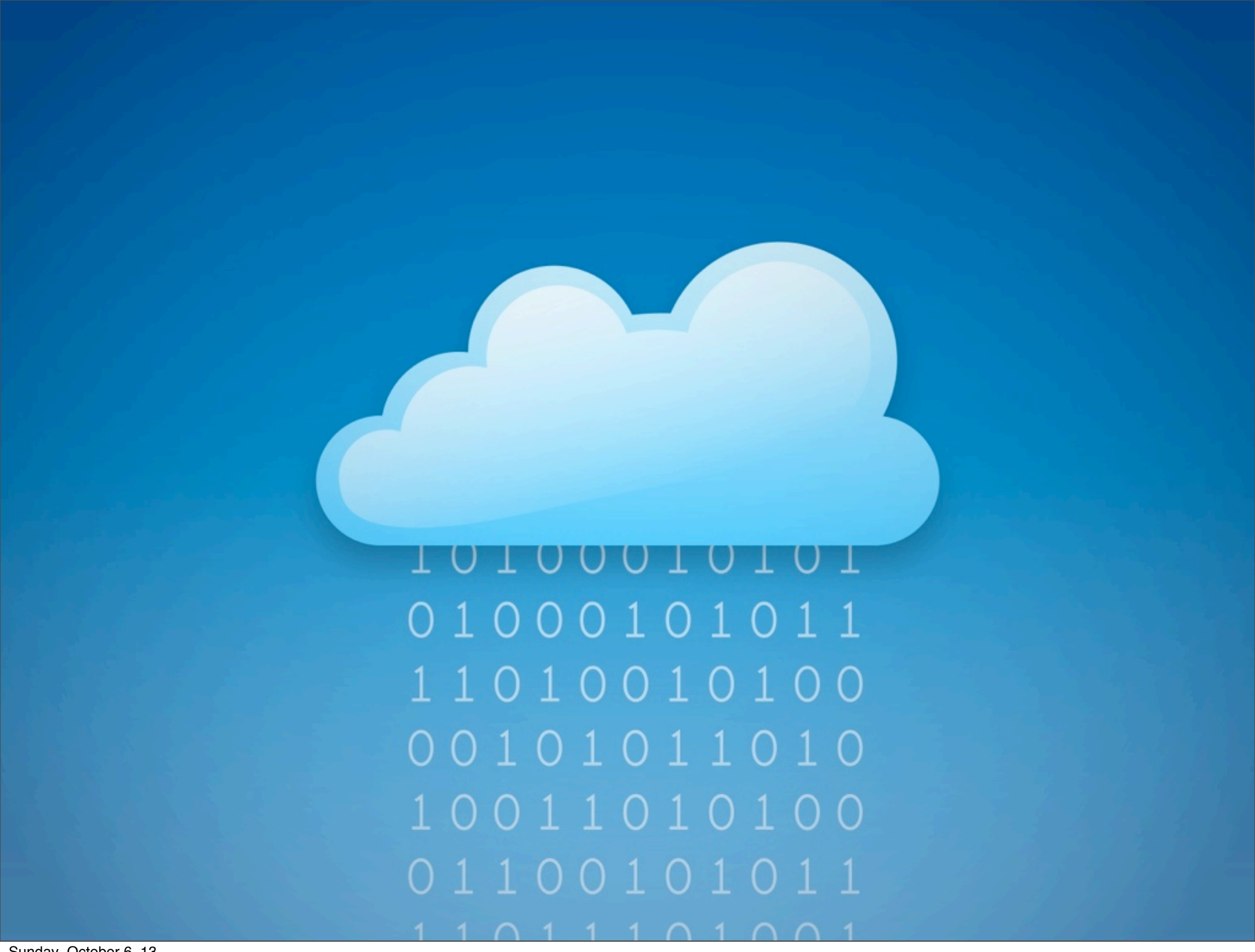
UI not as good



DIY: Do It Yourself

Dropbox

SkyDrive®


1 0 1 0 0 0 1 0 1 0 1
0 1 0 0 0 1 0 1 0 1 1
1 1 0 1 0 0 1 0 1 0 0
0 0 1 0 1 0 1 1 0 1 0
1 0 0 1 1 0 1 0 1 0 0
0 1 1 0 0 1 0 1 0 1 1

NAS

Network Attached Storage

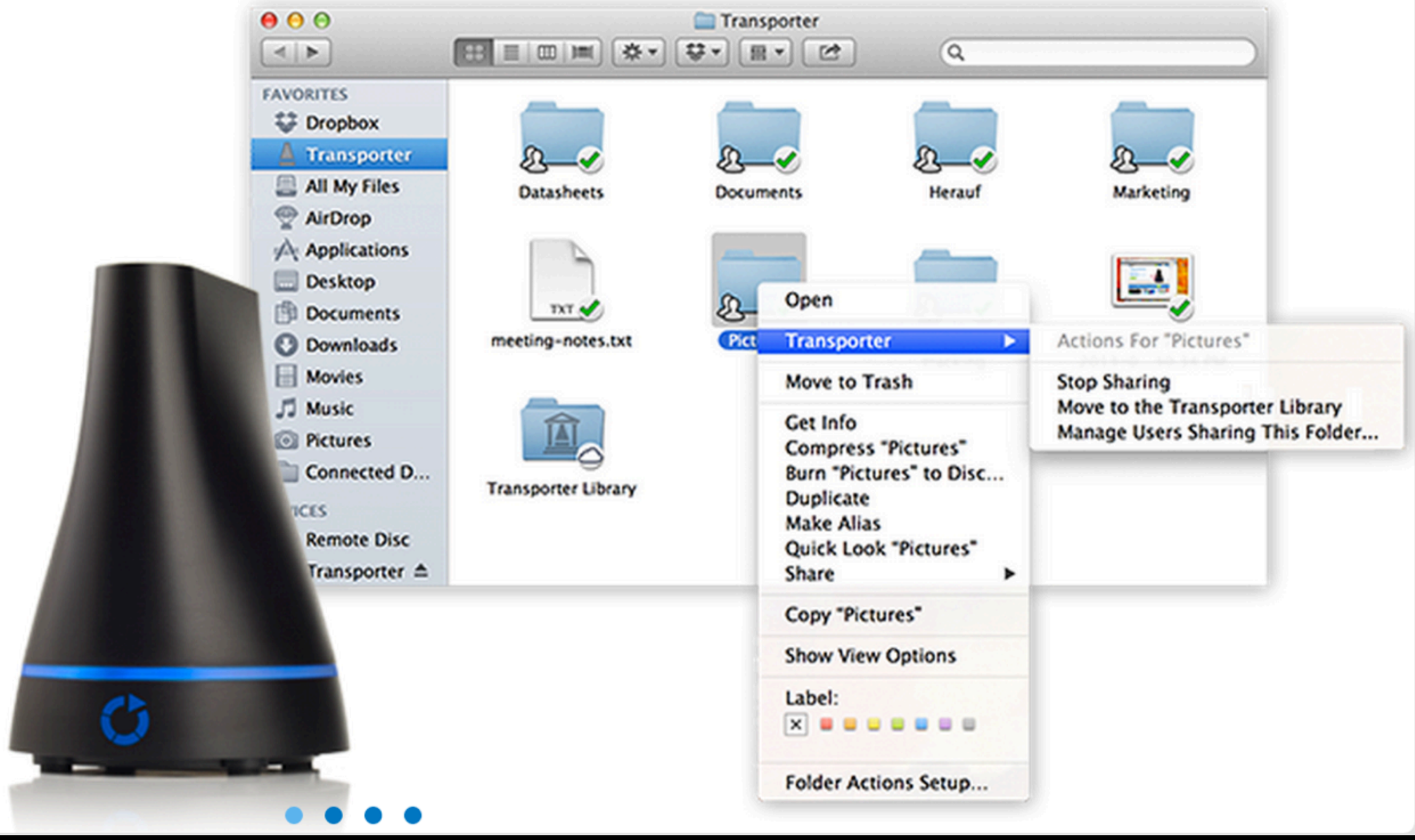
A small computer
with hard drives in it
that you control
& can access over the Net

Transporter by Connected Data

“Transporter is
a private cloud storage device
for syncing, sharing, accessing,
& protecting your digital life.
No cloud, no fees,
no privacy concerns.
Your files are only stored on your
Transporters & computers
& mobile devices that you authorize.”

2.0TB

5V


Transporter
FAVORITES
Dropbox
Transporter
All My Files
AirDrop
Applications
Desktop
Documents
Downloads
Movies
Music
Pictures
Connected D...
Remote Disc
Transporter
Datasheets
Documents
Herauf
Marketing
meeting-notes.txt
Transporter Library
Open
Transporter
Move to Trash
Get Info
Compress "Pictures"
Burn "Pictures" to Disc...
Duplicate
Make Alias
Quick Look "Pictures"
Share
Copy "Pictures"
Show View Options
Label:
Folder Actions Setup...
Actions For "Pictures"
Stop Sharing
Move to the Transporter Library
Manage Users Sharing This Folder...

Connected Folders
Apps
Available
Company
Available
Images
Available
Working
Available

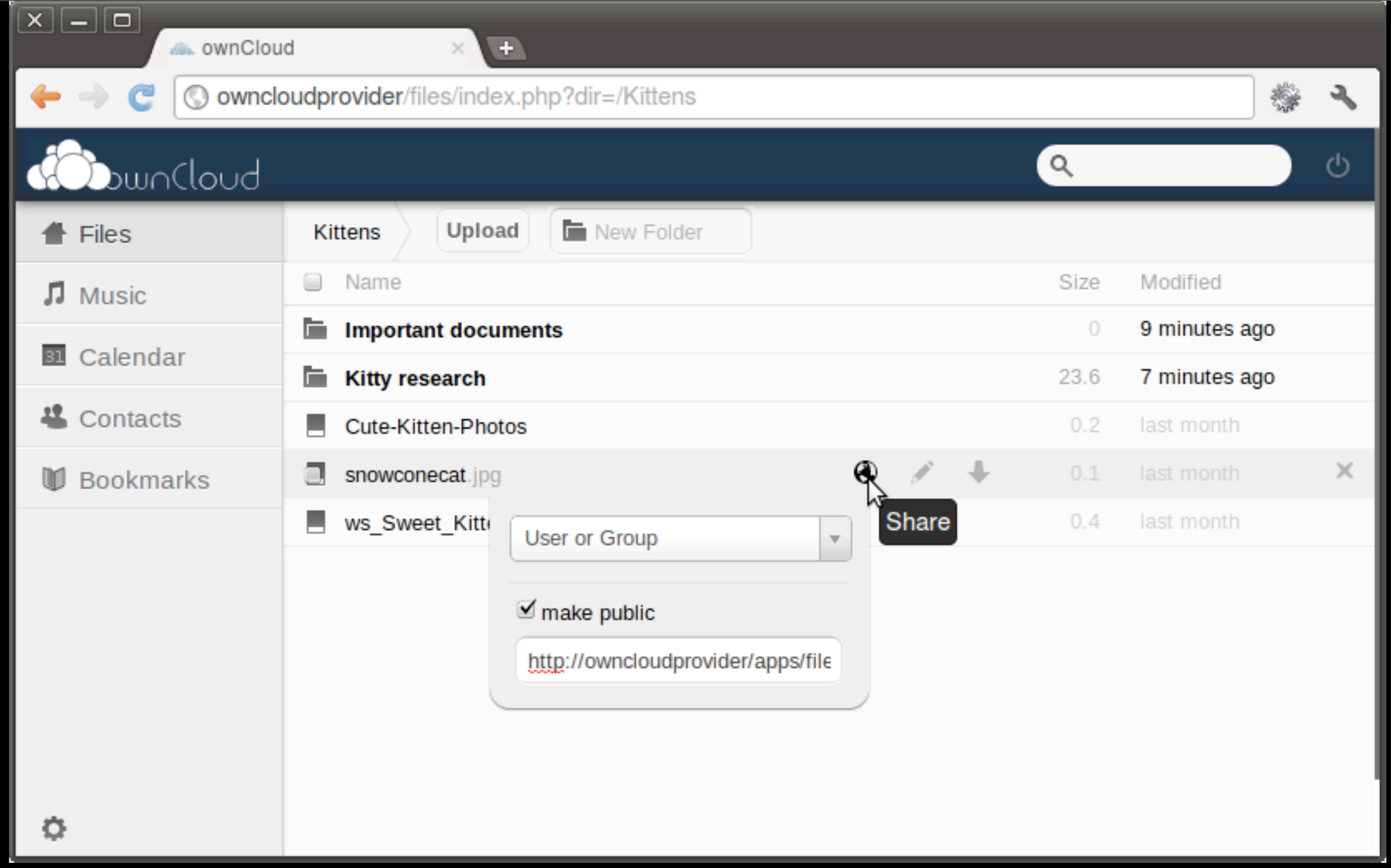
$190 without hard drive

$300 with 1 TB hard drive

$397 with 2 TB hard drive

www.filetransporter.com

ownCloud



File storage, versioning, syncing, & sharing

Contacts, calendars, photo galleries

Apps

Free & open source

owncloud.org

lifehacker.com/5993596/how-to-set-up-your-own-private-cloud-storage-service-in-five-minutes-with-owncloud

Synology®

STATUS
LAN
HDD 1
HDD 2
HDD 3
HDD 4
Synology
Synology
DiskStation DS413j

DC IN
LAN
USB
RST

- **Backup**
  - Desktop Backup
  - Time Backup
  - USBCopy & SDCopy
- **Easy Management**
  - Account & Privilege
  - Home Storage
- **File Sharing**
  - Cloud Station
  - File Station
  - FTP
  - Windows, Mac, Linux
- **Home Applications**
  - Audio Station
  - Download Station
  - iTunes Server
  - Media Server
  - Photo Station
  - Print Server
  - Video Station
- **Internet Connection**
  - Network Service
  - Quick Setup
- **Mobile Apps**
  - DS audio
  - DS cloud
  - DS download
  - DS file
  - DS photo+
  - DS video
  - Printing Solution

https://granneman.dyndns.org:5001/webman/index.cgi

SearchFocus | F | Ent | RSG | WS | Soc | G | lets | G-RSG | News | Save | Other Bookmarks

File Station

Control Panel

Package Center

DSM Help

Quick Start

Synology DSM 4.0

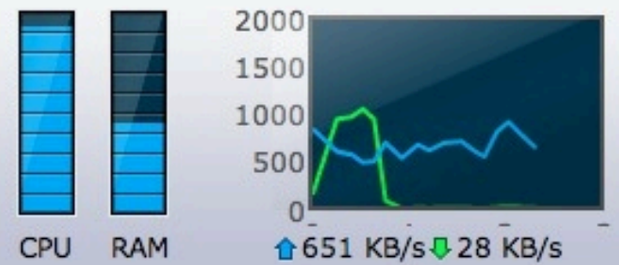
System Health

Good

Your DiskStation is working well.

Uptime: 81 day(s) 15:23:51

Resource Monitor



Recent Logs

1/5

- User [admin] logged in from [68.18...
- System successfully registered [71....
- Host [91.205.189.15] has been bloc...
- System successfully registered [71....
- Host [72.8.134.103] has been block...

https://granneman.dyndns.org:5001/webman/index.cgi

SearchFocus | F | Ent | RSG | WS | Soc | G | lets | G-RSG | News | Save | Other Bookmarks

File Station

Control Panel

Package Center

DSM Help

Quick Start

Control Panel

Search

File Sharing and Privileges

Win/Mac/NFS | FTP | WebDAV | User | Group | Shared Folder | Directory Service

Network Services

Web Services | ezCloud | Router Configuration | Firewall | Auto Block | Terminal | SNMP | Network Backup

System

Network | DSM Settings | Regional Options | Notification | Power | External Devices | Restore Defaults | DSM Update

Application Settings

Application Privileges | Application Portal | Mail Server | Syslog | VPN | Media Indexing Service

Synology DSM 4.0

https://granneman.dyndns.org:5001/webman/index.cgi#

https://granneman.dyndns.org:5001/webman/index.cgi

SearchFocus | F | Ent | RSG | WS | Soc | G | lets | G-RSG | News | Save | Other Bookmarks

File Station

Control Panel

Package Center

DSM Help

Quick Start

Package Center

Install / Update | Refresh | Settings

Installed | Available

Packages

Download Station
Status: Running
Stop
More

Media Server
Status: Stopped
Run
More

Surveillance Station
Status: Stopped
Run
More

Syslog Server
Status: Running
Stop
More

Photo Station
Status: Stopped
Run
More

Audio Station
Status: Stopped
Run
More

iTunes Server
Status: Stopped

Synology DSM 4.0

https://granneman.dyndns.org:5001/webman/index.cgi#

Government Agents

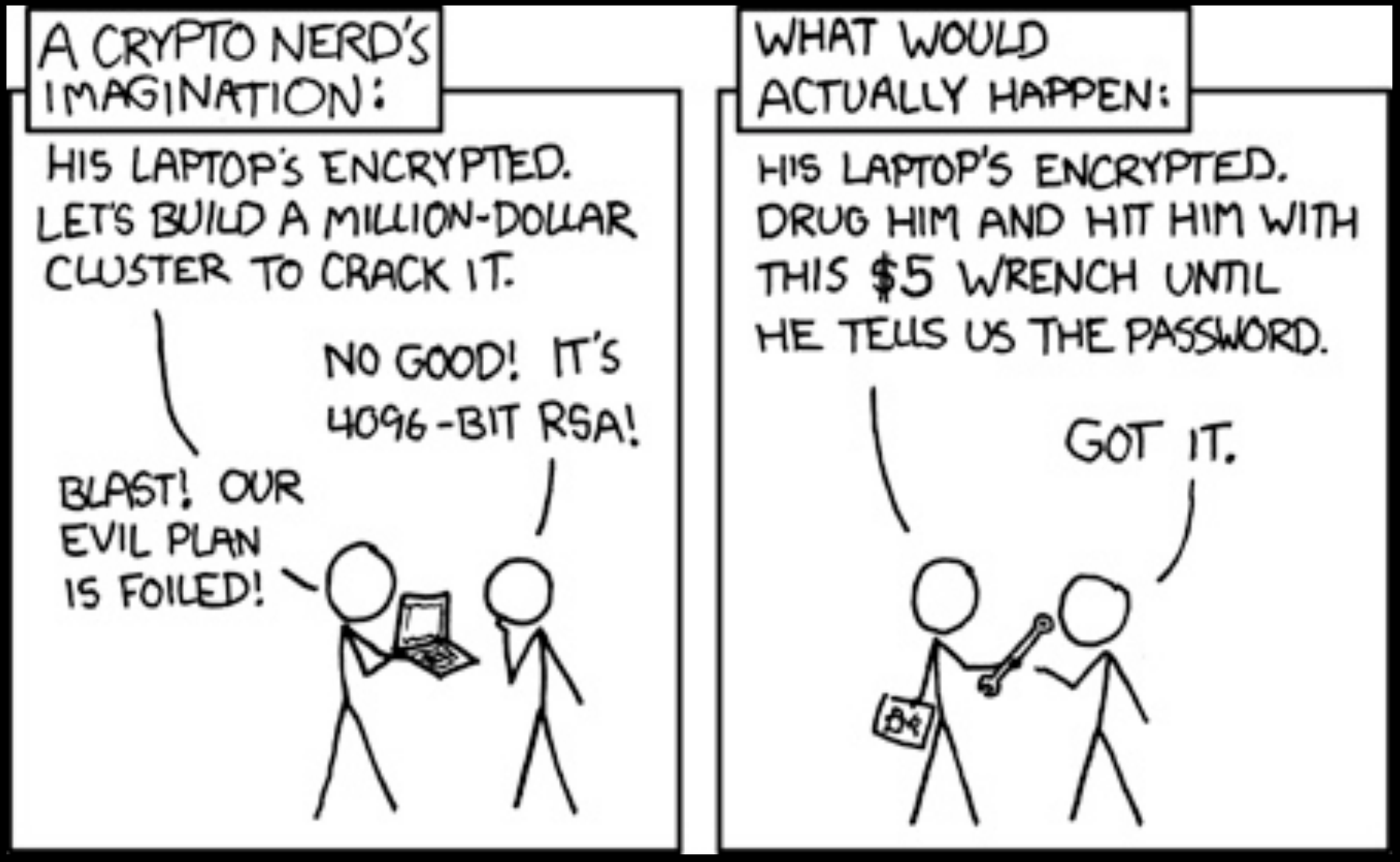
Any unencrypted message
sent over the Internet
is being delivered
to every intelligence service
in the world.

Edward Snowden,
August 13, 2013

The Goal:

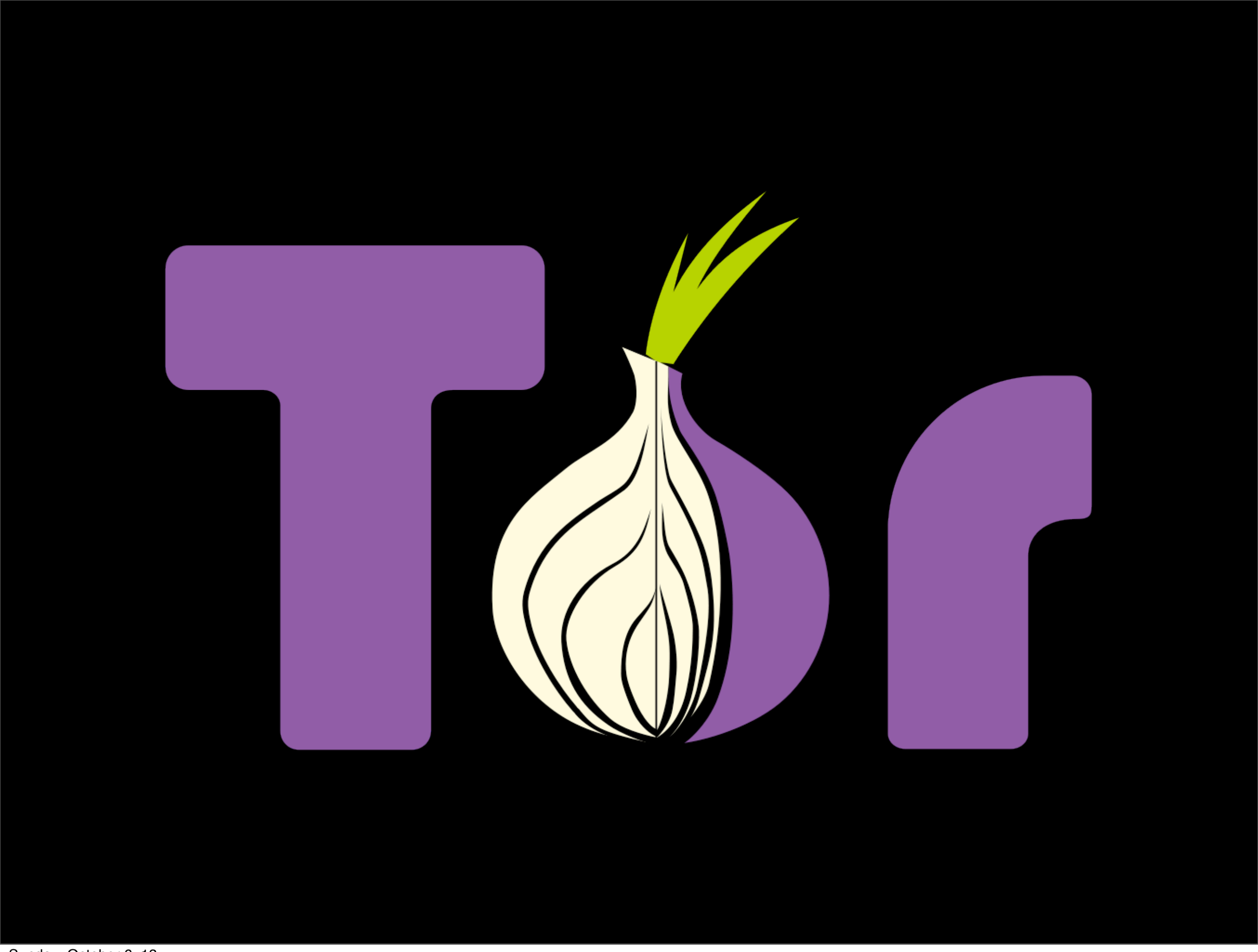
Protect your privacy
from the government

Also helps
against snoops & corporations



AKA, *rubber-hose cryptanalysis*

http://xkcd.com/538/

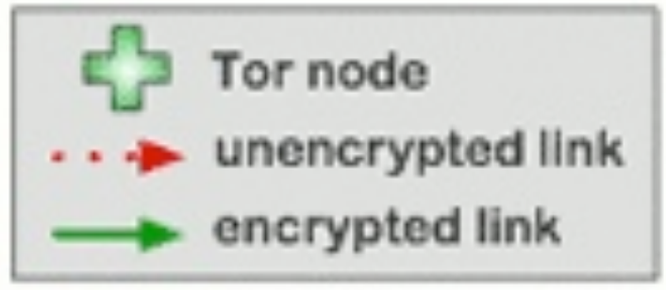

TOF

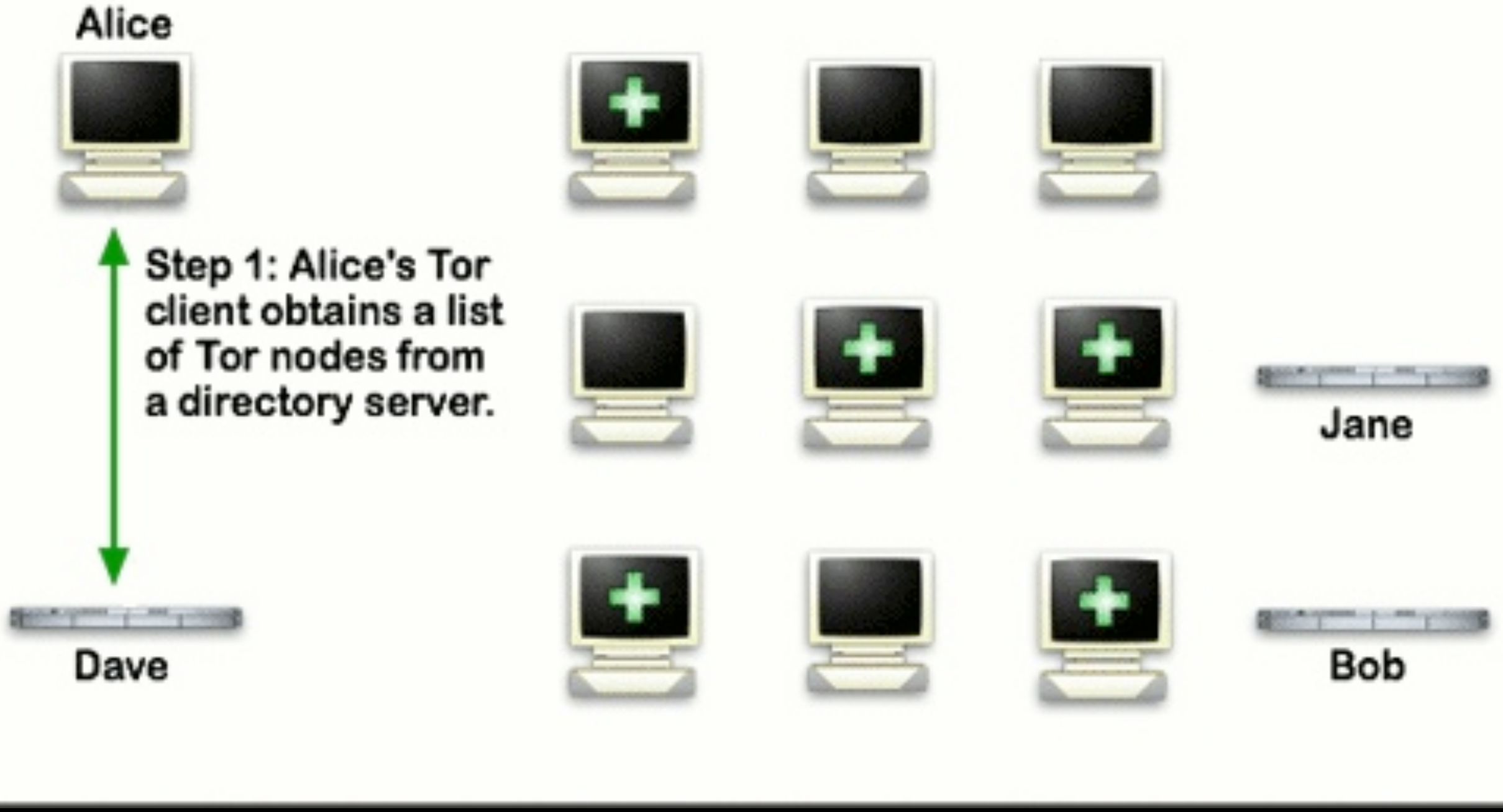
TOR

Onion routing

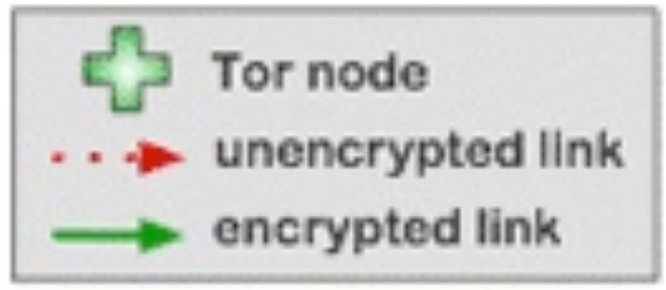
Hides
your Internet location & usage

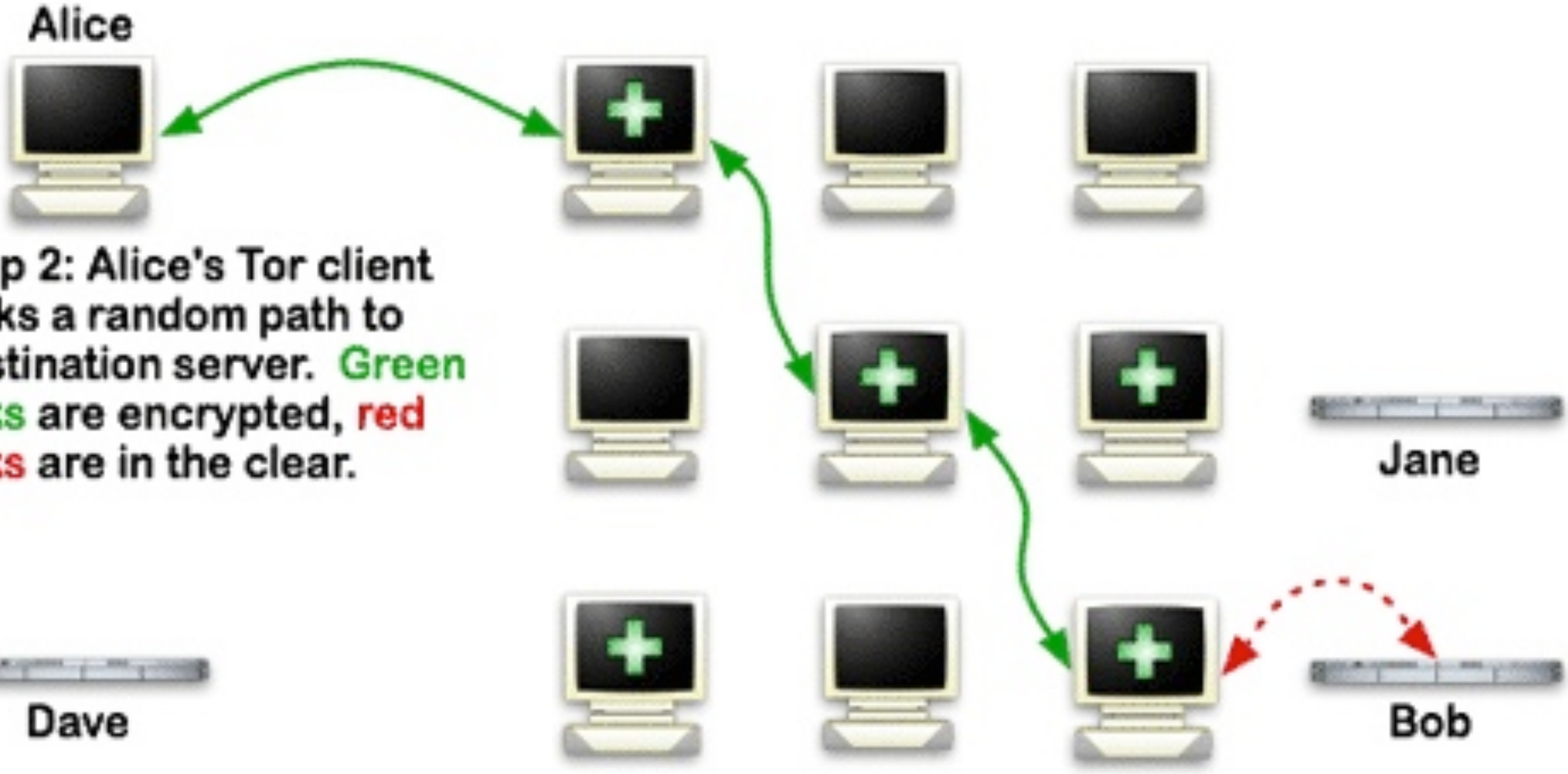
How Tor Works: 1



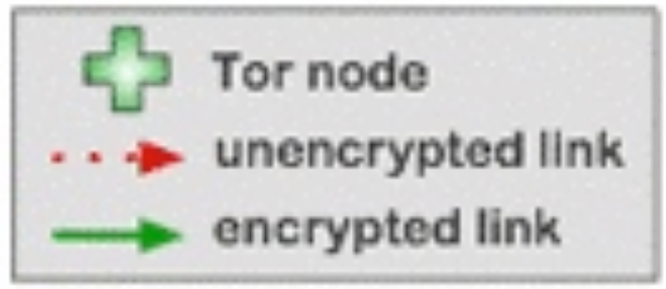


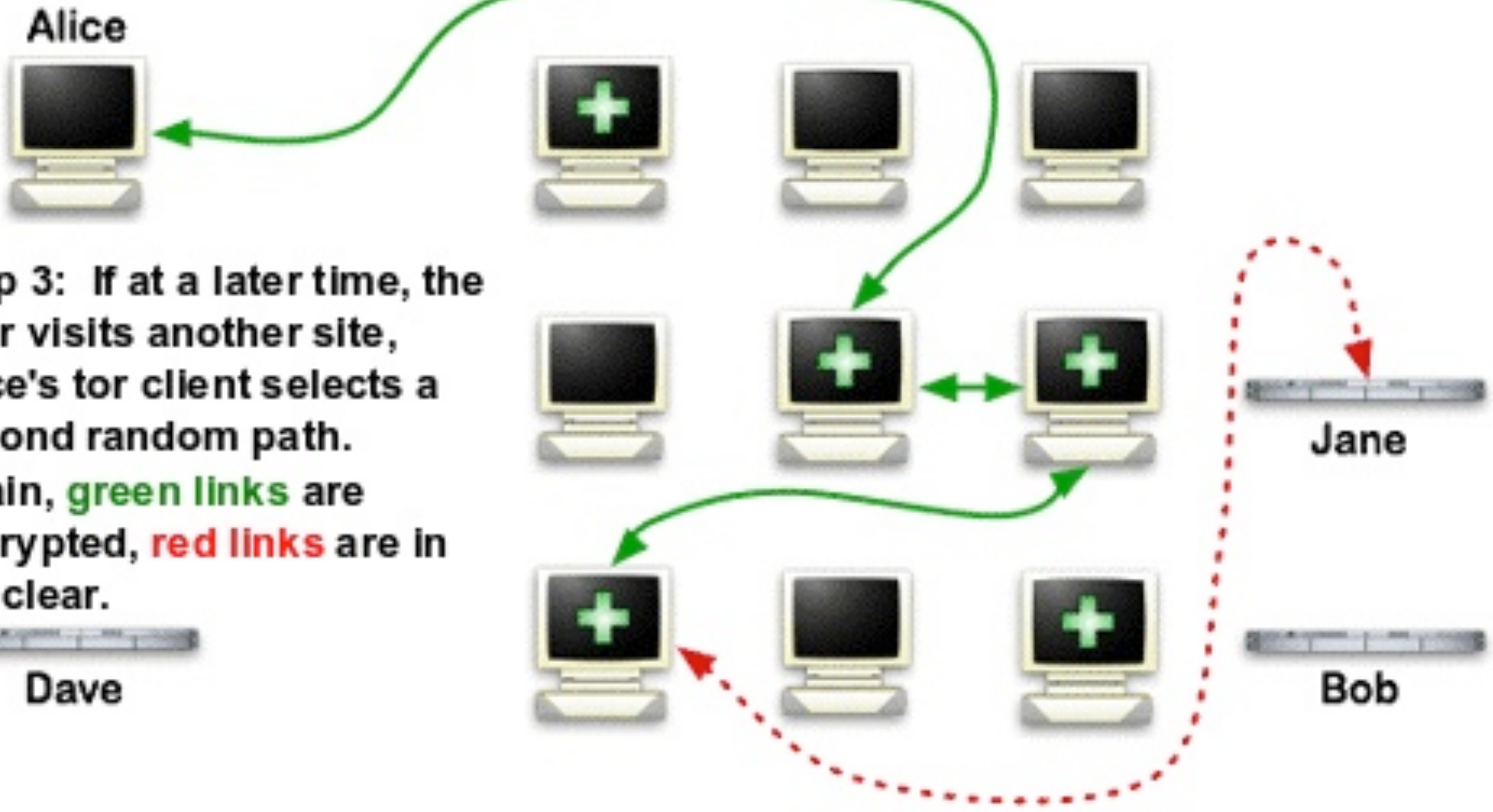
How Tor Works: 2





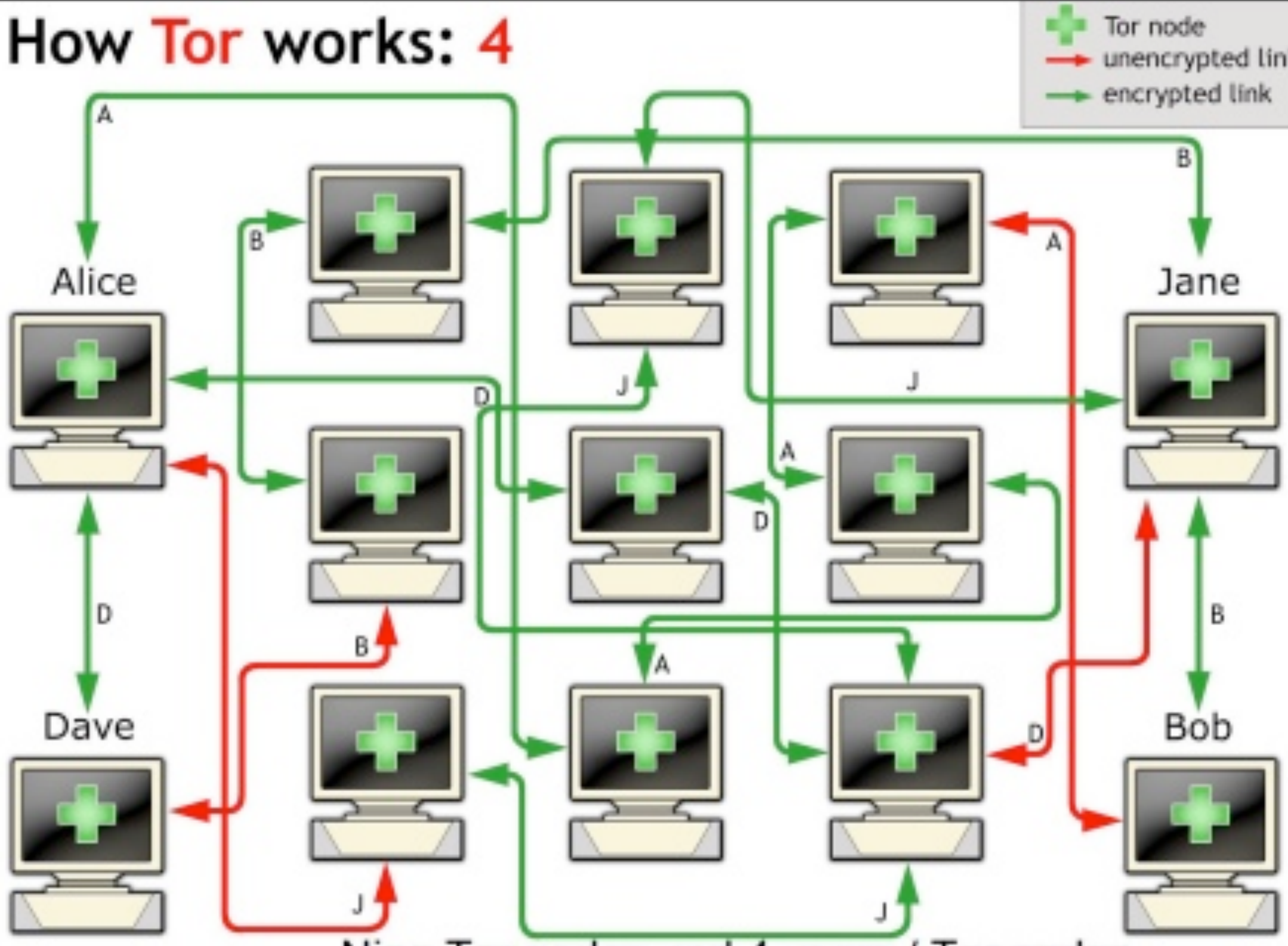
How Tor Works: 3





Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

How Tor works: 4



Nine Tor nodes and 4 users / Tor nodes

A: Alice connects to Bob - B: Bob connects to Dave

J: Jane connects to Alice - D: Dave connects to Jane

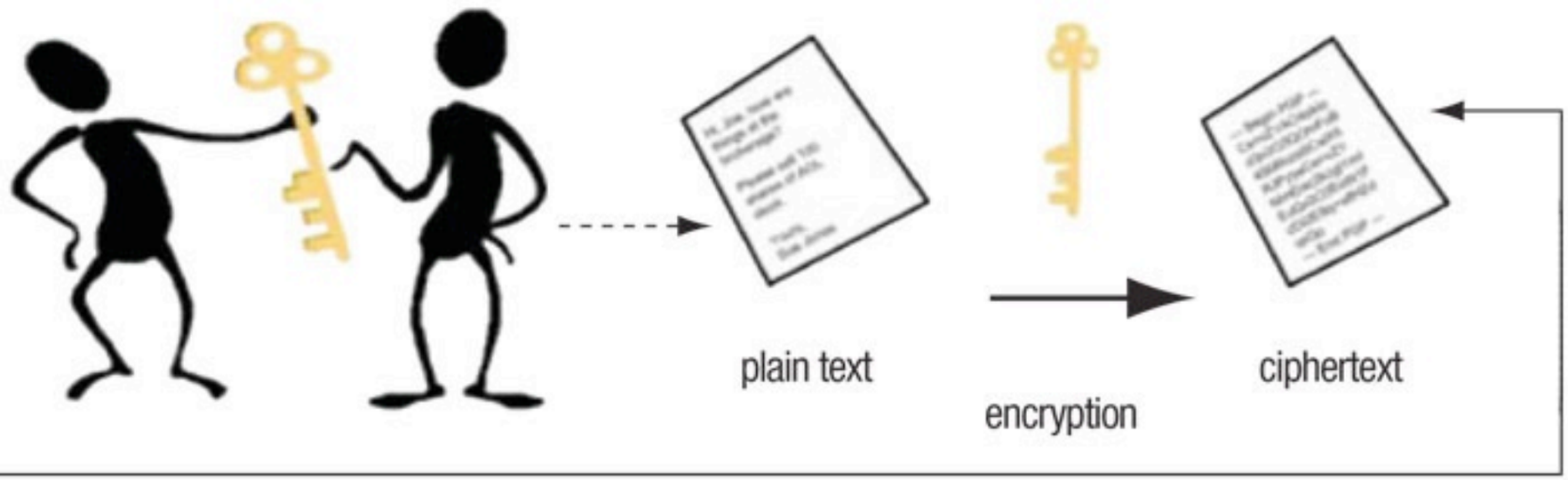
Slooooooow...

GnuPG

Public Key Encryption

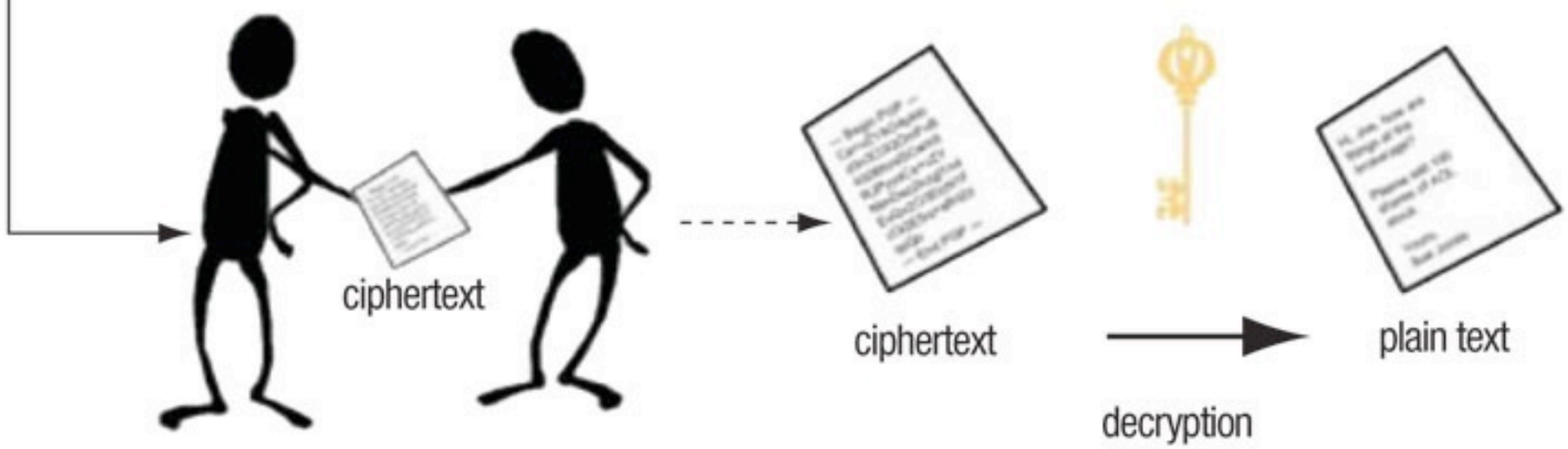
Step 1: Give your public key to sender

Step 2: Sender uses your public key to encrypt the plain text



Step 3: Sender gives the ciphertext to you.

Step 4: Use your private key (and passphrase) to decrypt the ciphertext.



Test mail

OpenPGP

To: GPGTools Core Team List

Cc:

Bcc:

Subject: Test mail

From: Steve… Signature: None

This mail will be encrypted and signed. I have both, the GPGTools public key, as well as my own secret key, in GPG Keychain Access.

Aha... this really works. :)

Great stuff. Enjoy safe communication with GPGTools.

--
http://support.gpgtools.org
http://gpgtools.org

Bruce Schneier:

“We’re already trying to phase out
1024-bit RSA keys
in favor of 2048-bit keys.
Perhaps we need
to jump even further ahead
and consider 3072-bit keys.”

The problems?

Everyone has to set it up

Everyone has to exchange public keys

Everyone has to use it

You can’t search your email or hard drive

Webmail doesn’t support it

S/MIME

Secure/Multipurpose
Internet Mail Extensions

2 services

✓ Digital signatures
✓ Message encryption

Advantages

✓ Much easier to use than GPG/PGP

✓ Email searchable

✓ Works with both
desktop & mobile clients
(& webmail)

Get your free cert

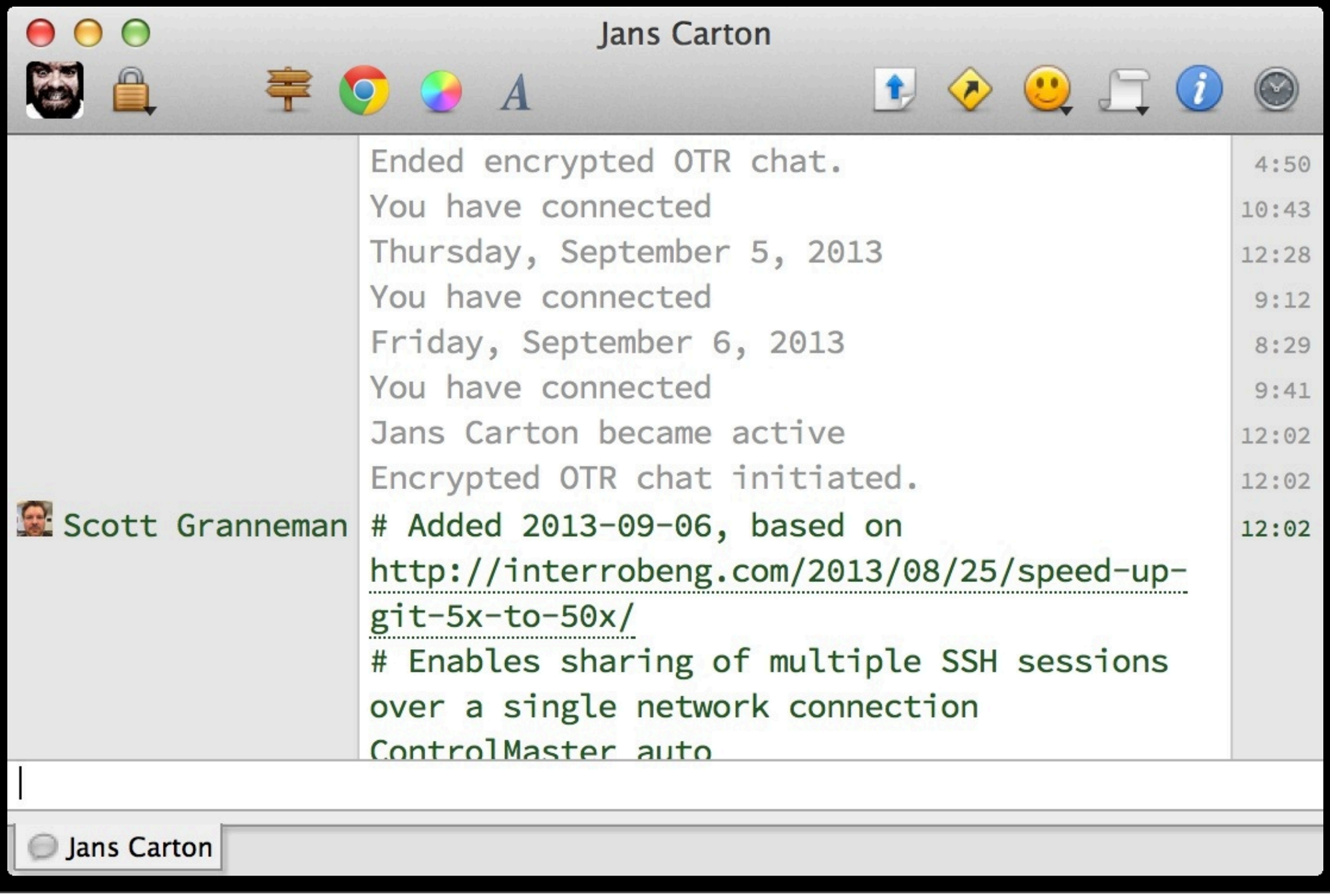
http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html

QTR

Off-the-Record Messaging

Encrypted IM

http://www.cypherpunks.ca/otr/s



IM clients
with built-in OTR

✓ Adium

✓ IM+

✓ Kopete

✓ Gibberbot

✓ Jitsi

IM clients
with OTR plugins

✓ Pidgin

✓ Miranda

✓ Trillian

✓ xchat

✓ Psi

“Air Gap”

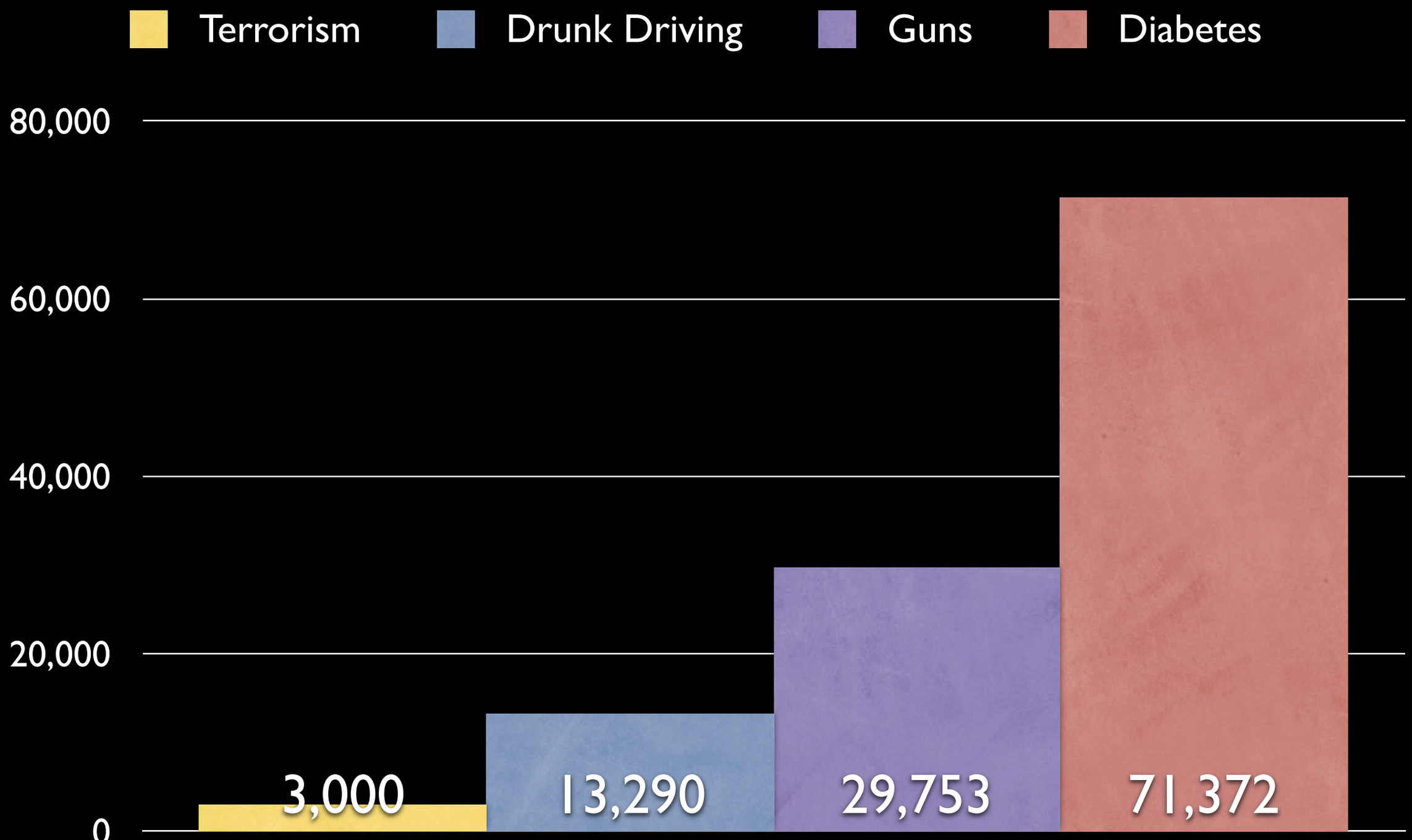
Bruce Schneier:

“Since I started working
with the Snowden documents,
I bought a new computer
that has never
been connected to the internet.

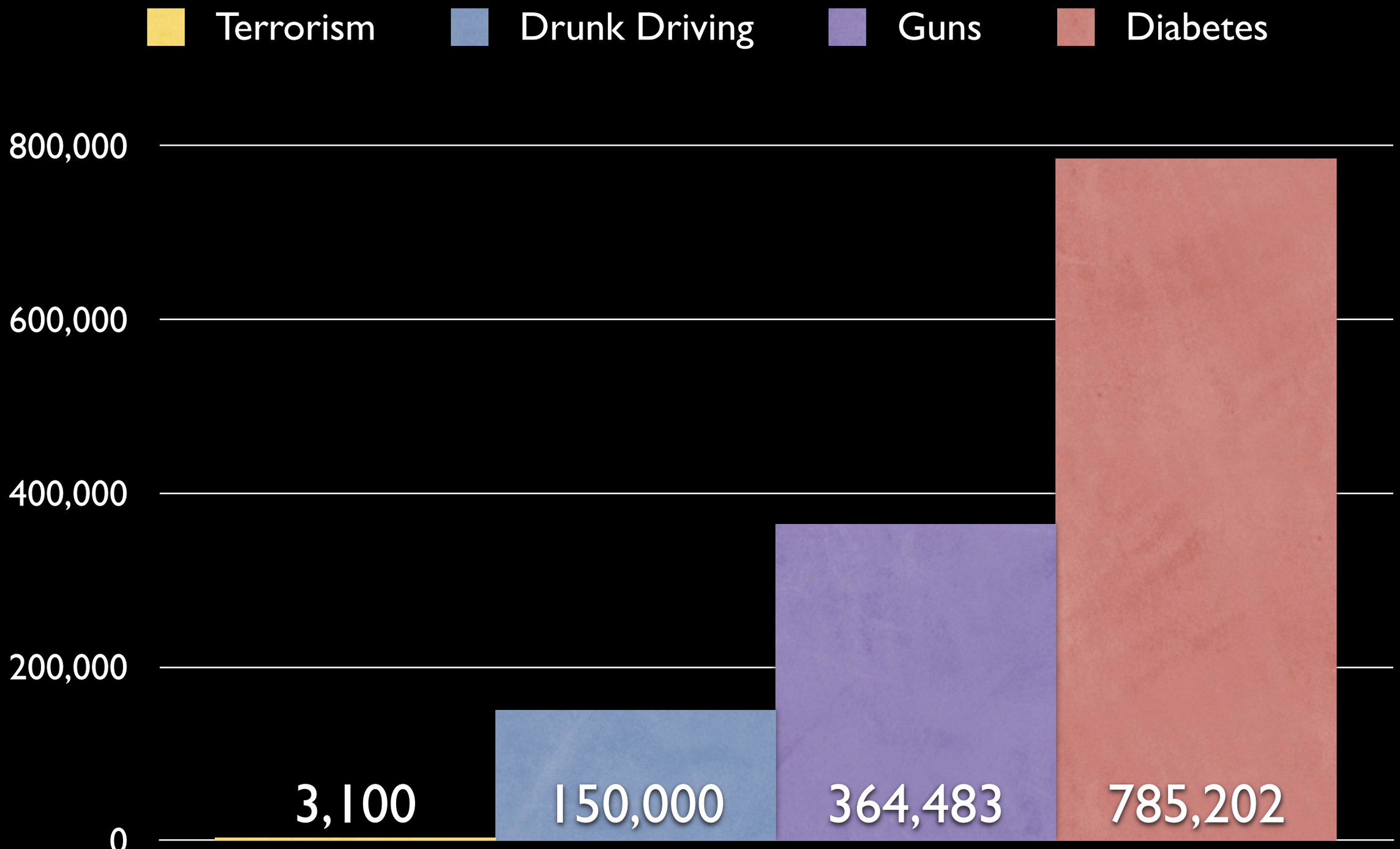
“If I want to transfer a file,
I encrypt the file
on the secure computer
and walk it over
to my internet computer,
using a USB stick.
To decrypt something,
I reverse the process.
This might not be bulletproof,
but it's pretty good.”

Objections

U.S. Deaths 2001



U.S. Deaths 1999–2010

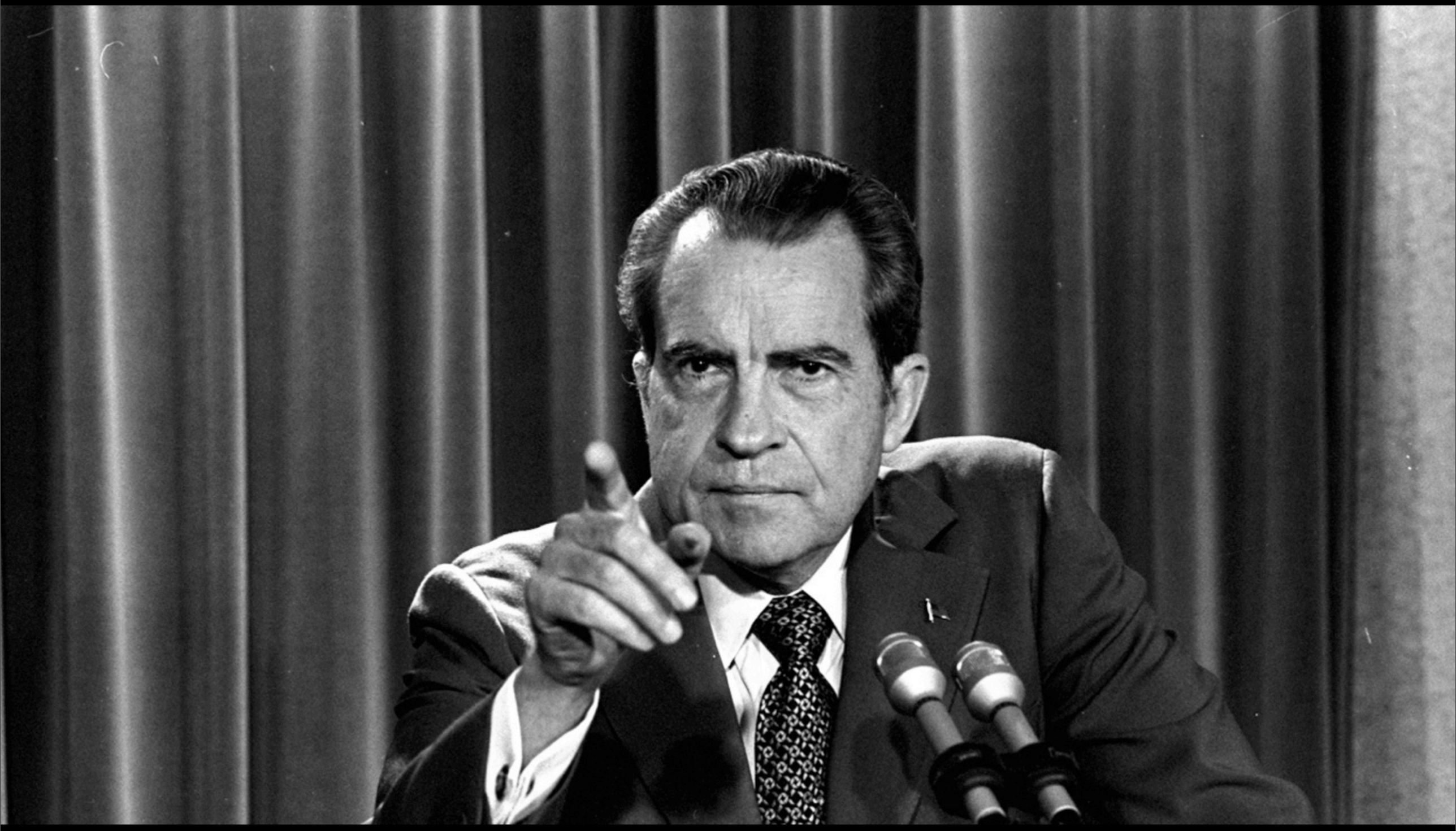


“If you’re not doing anything wrong,
then you shouldn’t mind
if the government watches you.”

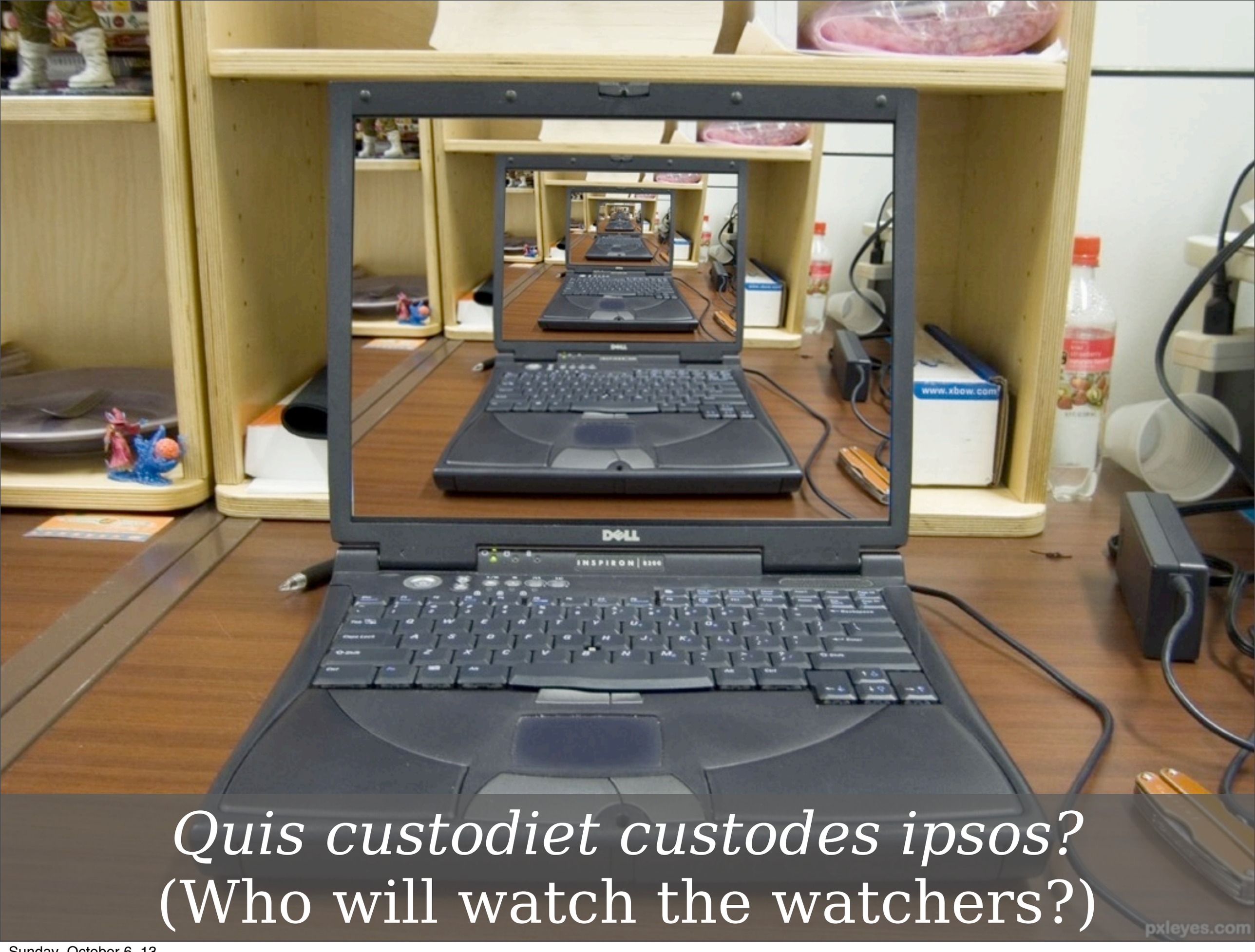
It’s not how you view yourself,
but how the government views *you*

It decides if you are a threat;
you don’t

Power corrupts



Absolute power corrupts absolutely



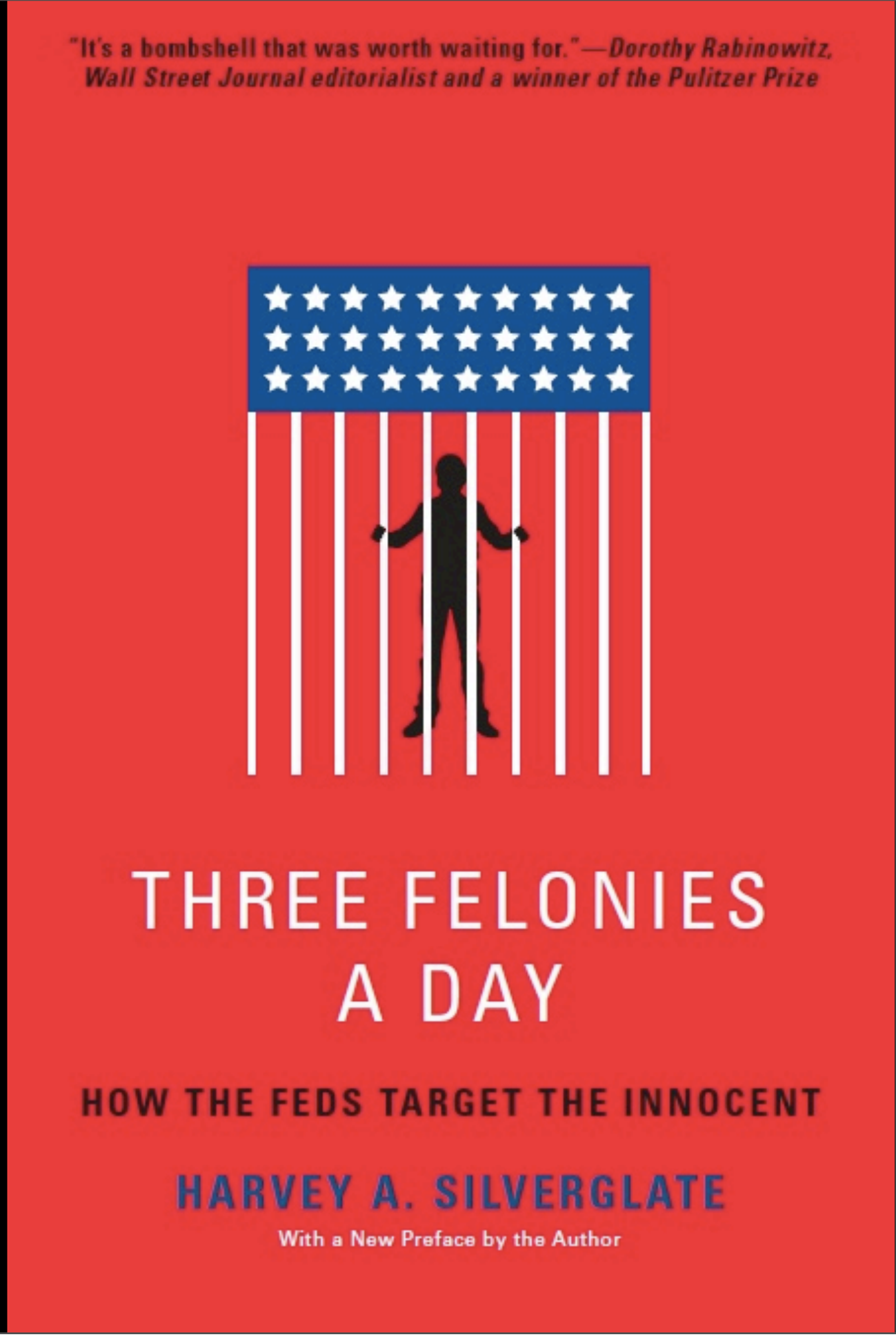
Quis custodiet custodes ipsos?
(Who will watch the watchers?)

Cardinal Richelieu:

"If one would give me six lines
written by the hand
of the most honest man,
I would find something in them
to have him hanged."

Forever is a long time

“[C]itizens who believe they are law-abiding may, in the eyes of federal prosecutors, be committing three felonies each day…”



DU

CONTRACT SOCIAL;

OU

PRINCIPES

DU

DROIT POLITIQUE.

PAR J. J. ROUSSEAU,

CITOYEN DE GENEVE.

— *fœderis æquas*
Dicamus leges.

Æneid. XI.

A AMSTERDAM,

Chez MARC MICHEL REY,

MDCCLXII.

Malo periculosam libertatem quam quietum servitium

(I prefer liberty with danger to peace with servitude)

Thank you!

Email: scott@granneman.com

Web: www.granneman.com

Publications: www.granneman.com/pubs

Blog: www.ChainsawOnATireSwing.com

Twitter: @scottgranneman

Email: denise@deniselieberman.com

What THEY Know, What YOU Don't:
Digital Intrusion & Digital Privacy

St. Louis UNIX Users Group

Scott Granneman
Denise Lieberman

© 2013 R. Scott Granneman
Last updated 20130911
You are free to use this work, with certain restrictions.
For full licensing information, please see the last slide/page.

POLICE DEPARTMENT

CITY OF PHOENIX, ARIZONA

SEARCH WARRANT

COUNTY OF MARICOPA, STATE OF A

NT NO.
2006-004692

TO ANY PEACE OFFICER IN THE STATE OF ARIZONA

Proof by affidavit having been made this day to me by Offi

I am satisfied that there is probable cause to believe th

[x] on person(s) of Suspect #1 Webster, Alan , black hair, brown eyes, 6'0", 185 lbs., Suspect #2 Webster, Nita M W/F, ir, brown eyes, 5'05", 120 lbs. and Suspect #3 Campbell, Joseph L. B/M , brown eyes, 6'02", 300 lbs.

[x] on the premises described as 250 e Flamingo Inn, #219. This being a multi unit motel complex constructed of n red trim. Apartment #219 is located in the south east corner of the building and is red in color with the number "219" on the door.

in the City of Phoenix e of Arizona, there is now being possessed or concealed certain property, persons o

Drug Paraphe

A usable amo a narcotic drug;

Firearms;

Indicia of occupancy, residency, and/or ownership of the premises described above, including, but not limited to utility, telephone bills, and canceled mail;

NO WARRANT