

# Cryptoparty Boston

Andrew Lewman  
andrew@torproject.org

09 February 2014





# George Orwell was an optimist

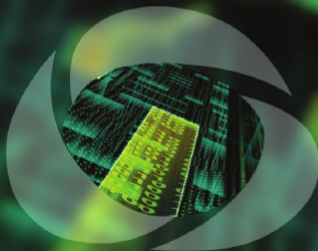


*Who controls the past, controls the future: who controls the present controls the past*

— George Orwell, Nineteen Eighty Four, 1949

# Internet Surveillance is getting more advanced

If You Can See It  
You Can **Monetize It**



Evolved DPI – See what's flowing through your network

# Internet Surveillance is getting more advanced

```
|0.541 | https > 50936 [SYN, (443)
| (50936) <-----
|0.541 | 50936 > https [ACK] (443)
| (50936) ----->
|0.542 | Client Hello (443)
| (50936) ----->
|1.030 | https > 50936 [ACK] (443)
| (50936) <-----
|1.033 | Server Hello, (443)
| (50936) <-----
|1.124 | 50936 > https [ACK] (443)
| (50936) ----->
|2.079 | [TCP Previous segme (443)
| (50936) <-----
|2.079 | [TCP Dup ACK 12#1] (443)
| (50936) ----->
|5.563 | [TCP Retransmission (443)
| (50936) <-----
|5.563 | 50936 > https [ACK] (443)
| (50936) ----->
|6.008 | [TCP Retransmission (443)
| (50936) <-----
|6.008 | 50936 > https [ACK] (443)
| (50936) ----->
|16.025 | Client Key Exchange (443)
| (50936) ----->
|17.533 | [TCP Retransmission (443)
| (50936) ----->
|20.735 | [TCP Retransmission (443)
| (50936) ----->
|21.127 | [TCP Previous segme (443)
| (50936) <-----
|26.447 | 50936 > https [FIN, (443)
| (50936) ----->
|26.743 | Encrypted Alert (443)
| (50936) <-----
|26.743 | 50936 > https [RST] (443)
| (50936) ----->
```

# Internet Surveillance is getting more advanced

## 'Comodo Hacker' Says He Acted Alone

**The plot thickens:** In an effort to back up his claims, alleged hacker dumps apparent evidence of pilfered database from breached Comodo reseller, as well as Mozilla add-on site certificate

By [Kelly Jackson Higgins](#) [InformationWeek](#)

April 09, 2011 12:00 AM

Comodo, a website certificate authority, revealed that nine SSL certificates were issued for fraudulent websites posing as domains for high-profile sites. Security researchers hope the incident will call attention to a certificate process they say is riddled with holes.

# Internet Surveillance is getting more advanced



5 Wednesday June 8, 2011, Francis Tan

## China increases Internet control, takes down hundreds of websites

China's government is coming out with new measures to control the ability of citizens to acquire domains and setup personal sites, and to block hundreds of sites that offer illegal downloads of music, films, and video games.

In what appears to be another upgrade of the government's [already strict control of the Internet](#), Chinese authorities contest that the stricter controls are intended to protect children from pornography, limit piracy, and to make it hard to perpetuate Internet scams.

Under the new controls, more than 700 pornographic and

### STORY TOOLBOX

[Tweet](#)



... Break the news

# Internet Surveillance is getting more advanced

## Major ISPs agree to "six strikes" copyright enforcement plan

By Nate Anderson | Published 9 months ago



American Internet users, get ready for ~~three strikes~~ "six strikes." Major US Internet providers—including AT&T, Verizon, Comcast, Cablevision, and Time Warner Cable—have just signed on to a voluntary agreement with the movie and music businesses to crack down on online copyright infringers. But they will protect subscriber privacy and they won't filter or monitor their own networks for infringement. And after the sixth "strike," you



# Internet Surveillance is getting more advanced

THE FUTURE OF PRIVACY FORUM  
WWW.FUTUREOFPRIVACY.ORG

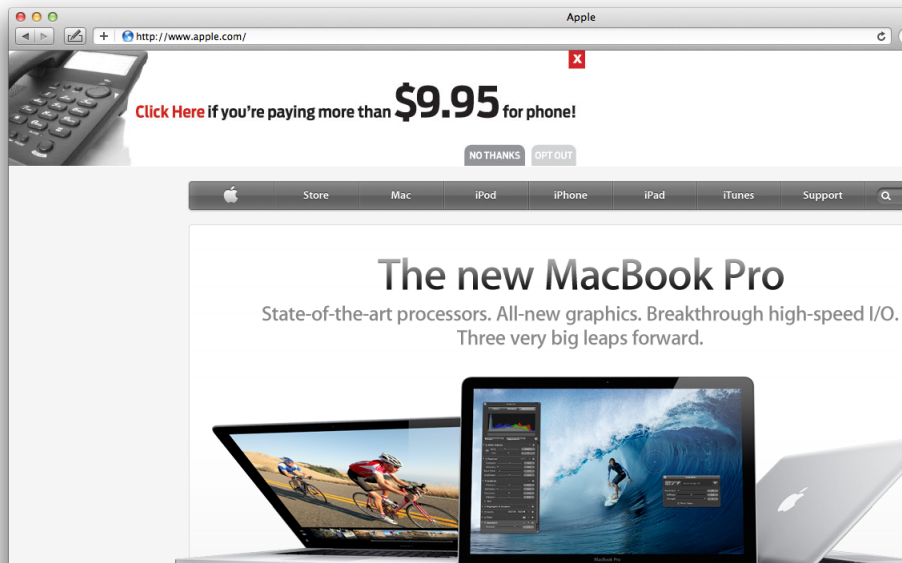


# Internet Surveillance is getting more advanced

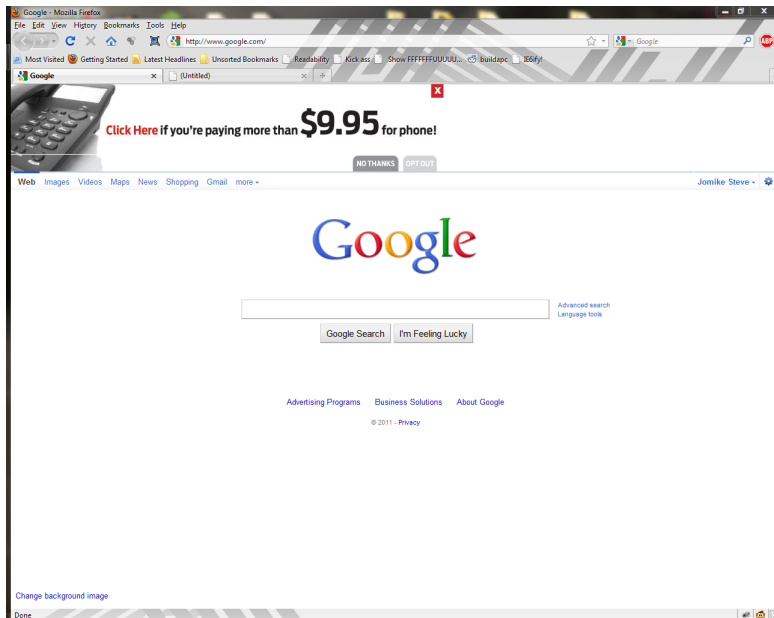
Tracker	Number of unique domains found on	Percent of all unique domains
Google Analytics	329,330	84%
Google Adsense	162,584	41%
DoubleClick	122,483	31%
Statcounter	26,806	7%
AddThis	24,126	6%
Quantcast	24,113	6%
Google Custom Search Engine	20,601	5%
OpenAds	17,608	4%
Omniure	13,126	3%
Wordpress Stats	11,475	3%

Figure 11 Percentage of Domains each Web bug was found on, March 2009

# Internet Surveillance is getting more advanced



# Internet Surveillance is getting more advanced



## Iran Protests: Twitter, the Medium of the Movement

By LEV GROSSMAN Wednesday, Jun. 17, 2009

### Related

#### Photos



Behind the Scenes  
with Mousavi

#### Stories

- In Iran, Rival Regime Factions Play a High-Stakes Game of Chicken
- Latest Tweets on Fallout from Iran's



Share

The U.S. State Department doesn't usually take an interest in the maintenance schedules of dotcom start-ups. But over the weekend, officials there reached out to Twitter and asked them to delay a network upgrade that was scheduled for Monday night. The reason? To protect the interests of

# Twitter in USA: Bad.

## FBI Raids Queens Home in G20 Protest Twitter Crackdown



AP Photo/Matt Rourke

That's right, a Twitter crackdown. A lawyer for Jackson Heights social worker Elliot Madison, 41, says that the feds searched his client's house for 16 hours on Thursday after Madison was arrested on September 24th at a Pittsburgh hotel room with another man. What were they up to? Sitting at laptops sending Twitter messages advising [G20 demonstrators](#) about riot police activity in the streets. And yet *real* Twitter threats like [Lindsay Lohan](#) and [Courtney Love](#) remain at large.

Madison, a self-described anarchist, was in Pittsburgh volunteering for the [Tin Can Comms Collective](#), a group that uses Twitter to send mass text messages during protests describing events observed on the streets or over police scanners; stuff like "SWAT teams rolling down 5th Ave." Tin Can was active during the [St. Paul RNC protests](#), and the authorities are now on to them. Madison was charged with hindering apprehension or prosecution, criminal use of a communication facility and possession of instruments

of crime; he's currently out on bail.

from [http://gothamist.com/2009/10/05/fbi\\_raids\\_queens\\_home\\_in\\_g20\\_protes.php](http://gothamist.com/2009/10/05/fbi_raids_queens_home_in_g20_protes.php)



# The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy





# What is Tor?

- online anonymity software and network

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:

Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT, NORDUnet...

# What is Tor?


- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:  
Drexel, Univ of Waterloo, Georgia Tech, Princeton, Boston University, University College London, Univ of Minnesota, National Science Foundation, Naval Research Labs, Cambridge UK, Bamberg Germany, MIT, NORDUnet...
- increasingly diverse toolset:  
Tor, Tor Browser Bundle, Tails LiveCD, Pluggable Transports, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Gibberbot, Arm and so on.

# Why Tor?

*FIRST RULE OF PRIVACY*

***I am the only one who can  
decide what I want to share.***

# Why Tor?



`./images/internet-venn-diagram.jpg`

# Who uses Tor?



- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

# Online and Offline change happens





# You missed a use case

`./images/hidden-service-takedown-warning.jpg`

# You missed a use case



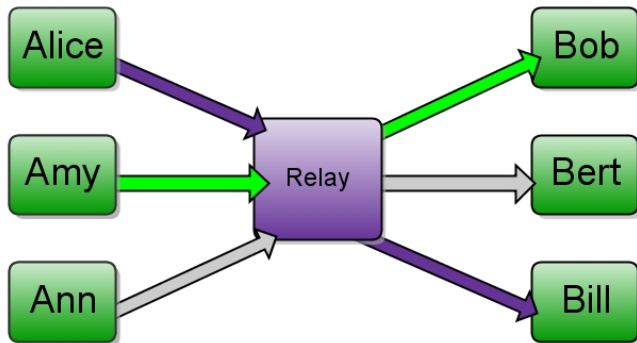
# You missed a use case



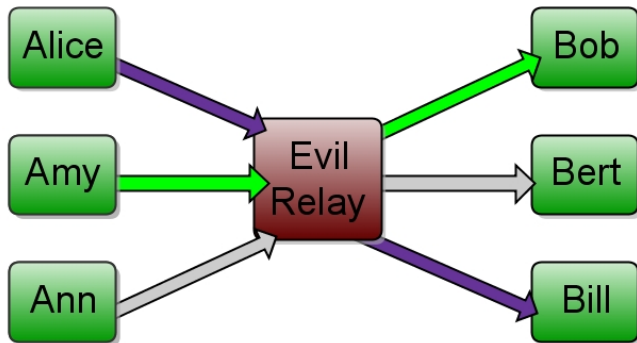
estimated 1 million daily users



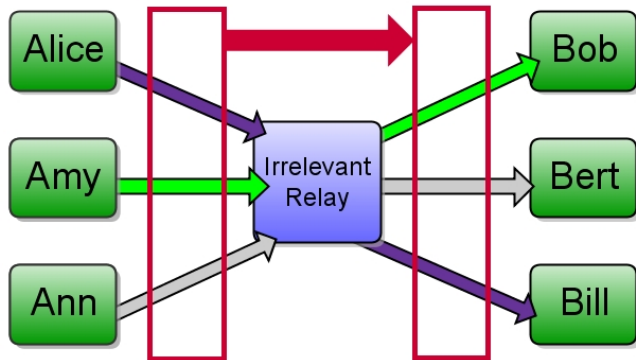
# How is Tor different from other systems?



## How is Tor different from other systems?



## How is Tor different from other systems?



# Tor hides communication patterns by relaying data through volunteer servers

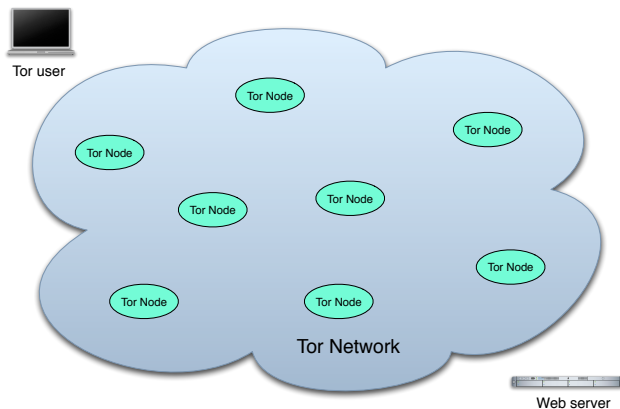


Diagram: Robert Watson



# Tor hides communication patterns by relaying data through volunteer servers

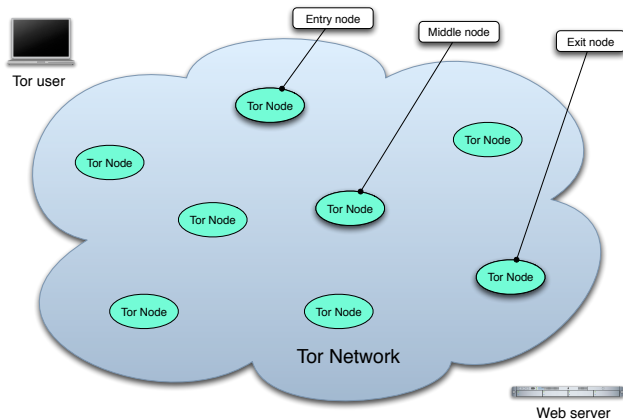


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers

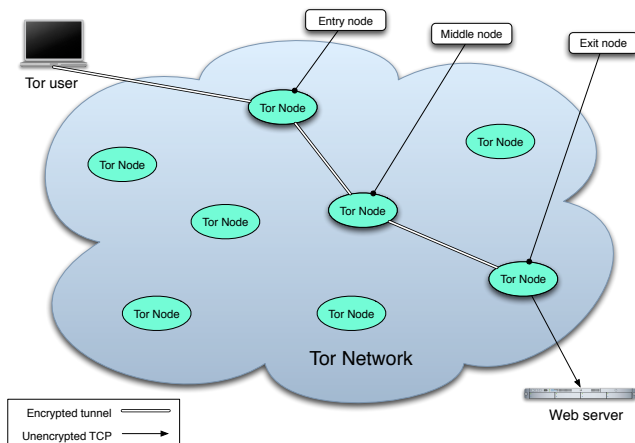


Diagram: Robert Watson

# Tor hides communication patterns by relaying data through volunteer servers

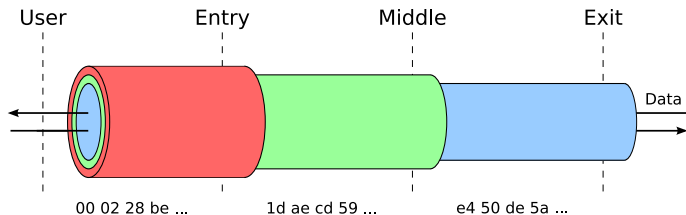
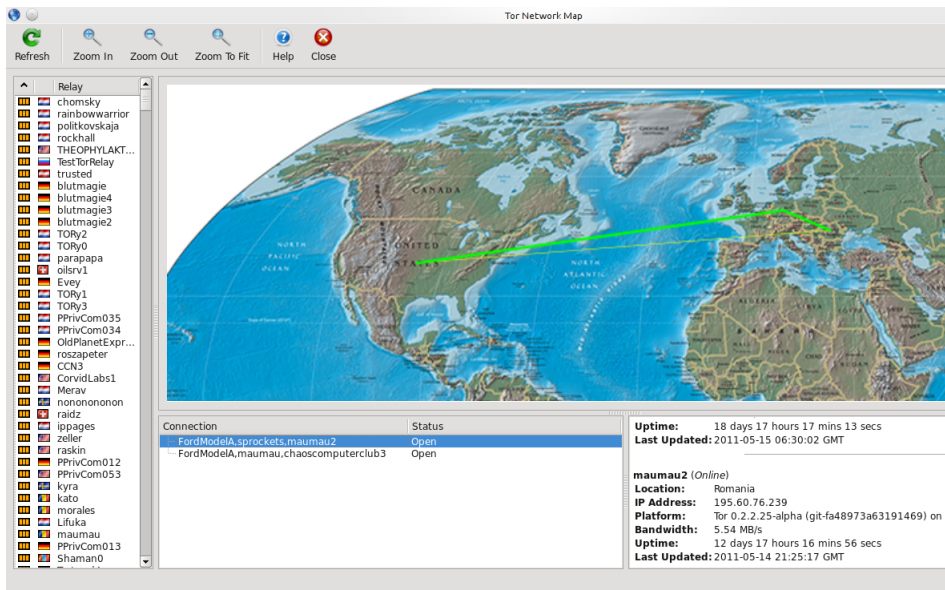


Diagram: Robert Watson

# Vidalia Network Map



# Metrics

- Measuring metrics anonymously
- NSF research grant
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal:  
<https://metrics.torproject.org/>

# Tor hidden services allow privacy enhanced hosting

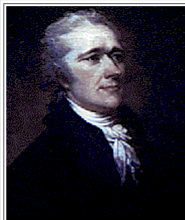


The Federalist - Contents - Namoroka

File Edit View History Bookmarks Tools Help

http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm

The Federalist - Contents



Alexander Hamilton



James Madison

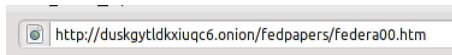


John Jay

## The Federalist

The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuation errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", s have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are the edition used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are in original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the newspapers were the *Independent Journal* [J], the *New-York Packet* [P], and the *Daily Advertiser* [A], all based in New York. The first paper actually first appeared May 28, 1788, in a bound volume published by J. and A. McLean, *Federalist II*. We have followed each paper to its primary author: James Madison [M], John Jay [J], or Alexander Hamilton [H], which is shown following the text.

dot onion you say?



Thanks!



Visit <https://www.torproject.org/> for more information, links, and ideas.



## Credits & Thanks

- applied theory, third image: Information Week, 2011-04-09, <http://www.informationweek.com/news/security/attacks/229400850>
- applied theory, fourth image: Al Jazeera, February 2011
- six strikes, ars technica, <http://arstechnica.com/tech-policy/news/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plaintiffs-ars>
- spring is in the air, Paco Pomet, <http://pacopomet.wordpress.com/>
- who uses tor? <http://www.flickr.com/photos/mattw/2336507468/sizes/o/>, Matt Westervelt, CC-BY-SA.
- danger!, <http://flickr.com/photos/hmvh/58185411/sizes/o/>, hmvh, CC-BY-SA.
- 1 Million, <http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/>, Luka Skracic, used with permission.