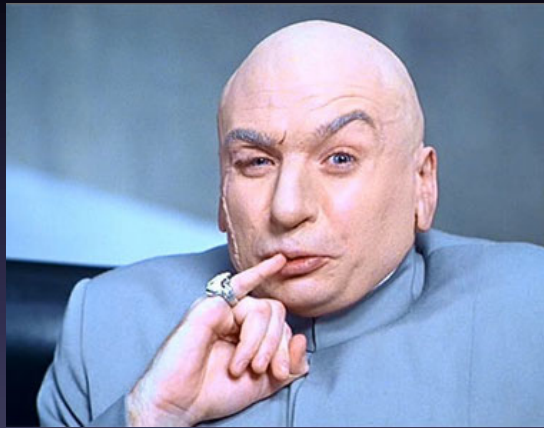


why should you care  
about encryption?



when you're not doing anything  
wrong or illegal

# about me

name: Shawn Maxim



specialties: vulnerability assessment , mitigation/  
remediation, and security policy compliance

experience: Federal Reserve, consulting, Apple

education: BS in CS at CSUS focus on CyberSecurity

more info: [shawnmaxim.net](http://shawnmaxim.net) & [etherealsolid.com](http://etherealsolid.com)

# agenda

- definitions
- problem
- background
- solutions
  - general
  - communication
  - web browsing



# privacy

/ˈprɪvəsi/

*noun*

the state or condition of being free from being  
observed or disturbed by other people

# confidential

\|kän-fə-'den(t)-shəl\

*adjective*

- secret or private
- showing that you are saying something that is secret or private
- trusted with secret or private information

# is there a right to privacy in the US?

The right to privacy is not mentioned in the Constitution, but the Supreme Court has said that several of the amendments create this right. The Fourth Amendment stops the police and other government agents from searching us or our property without "probable cause" to believe that we have committed a crime. Other amendments protect our freedom to make certain decisions about our bodies and our private lives without interference from the government.

# is there a problem here?

should you be concerned about your privacy?

what about the confidentiality of your personal  
information?



# background: who?



who wants our data?

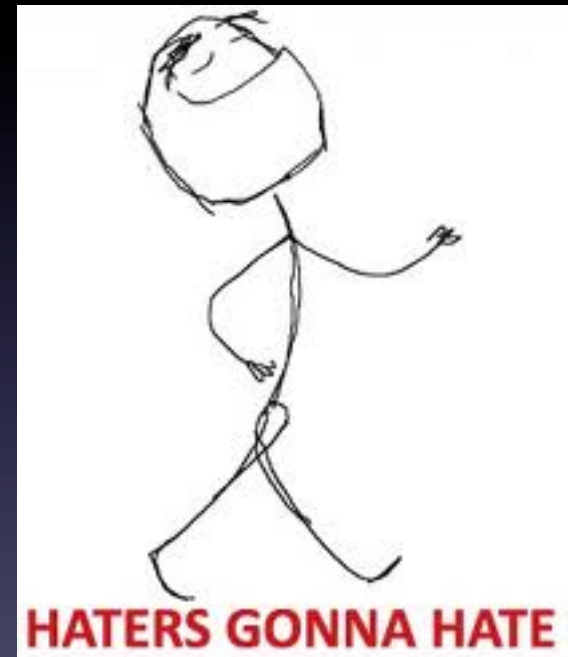
- governments
- corporations and companies
- criminal groups



# background: why?

why is data so valuable?

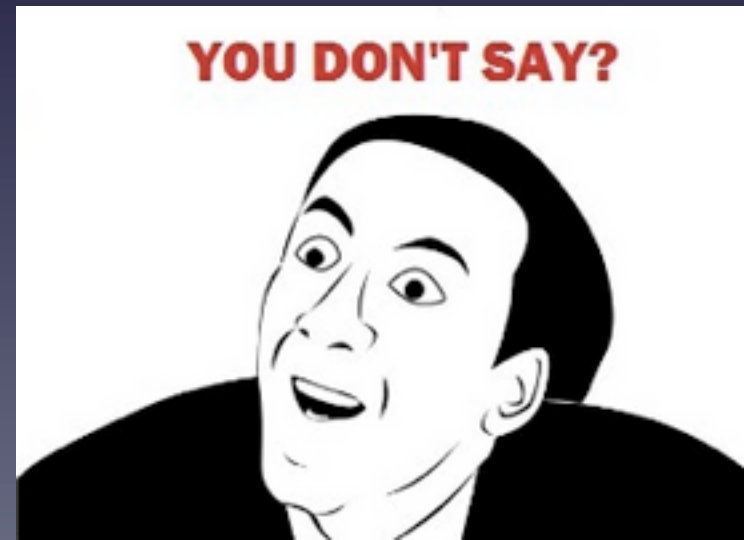
- monetization
  - targeted advertising
  - data aggregation services
  - criminal activity
- surveillance programs
- behavioral analysis



# background: what?

what data is valuable?

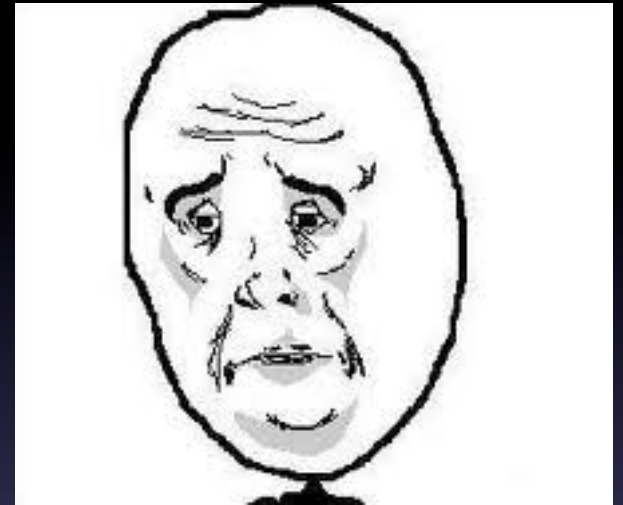
- browsing and purchasing tracking
- content of communications
- personal information
- financial information



# background: where?

where is the data gathered?

- web browsing
- ISPs
- wireless providers
- companies handling communications
- exploited systems
- taps owned by “interested parties”



# background: how?

how is this data gathered?

- web browsing
  - cookies, sessions, unique ID's, credentials, fingerprinting
- communications
  - logged information from: calls, SMS, emails, IMs, chats
- collection activity
  - breaches, surveillance, taps, standard logging and collection

# background: when?

when is the data being gathered?

- whenever you use the internet
  - browsing
  - communicating

# so what can we do?

remember: encryption is your friend!



privacy and confidentiality are achieved using  
secure processes and tools

# the most general advice

## think about your choices

- what are the ramifications for:
  - data sharing
  - privacy (or lack thereof)
  - confidentiality



# general solutions

- don't use unsecured wifi
  - unless you also are using VPN or other secure tunneling
- watch for data leakage
  - mobile app permissions
  - terms and conditions involving data use



# communication solutions

do you like to chat? text? instant message?

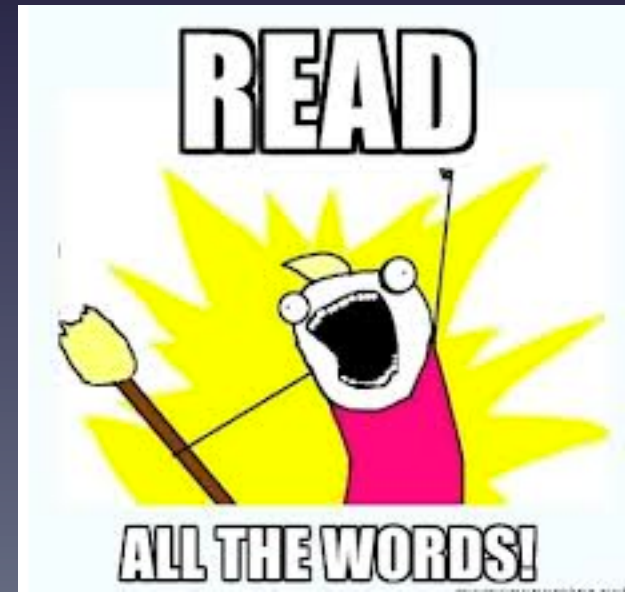
use a secure option with end to end encryption

- bleep (from BitTorrent for android, iOS, mac, PC)
  - [www.bleep.pm](http://www.bleep.pm)
- iMessage (mac and iOS)
- Tor messenger (still in beta, source code also available)

# browsing

think before you open that browser

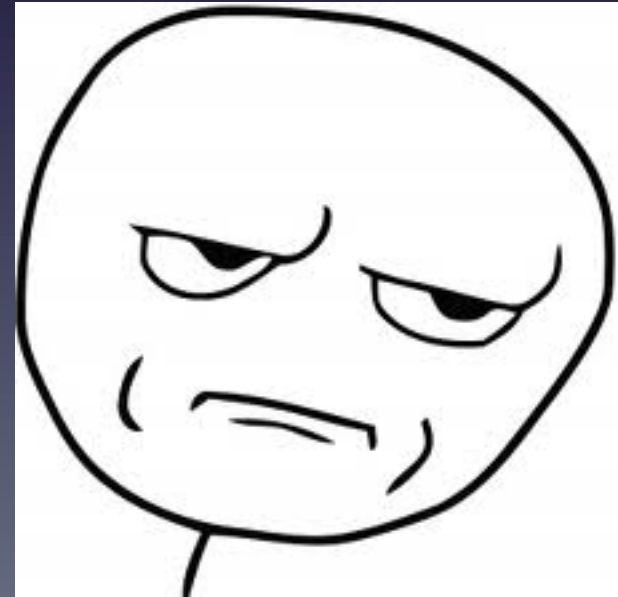
- who wrote it and where did you get it?
- how do they collect data and what is collected?
  - what did the terms and conditions say?



# browser facts

what data is leaking while browsing?

- sites you visited
  - what you looked at while you were there
- where you are located
- what software you are using
- your computers 'fingerprint'



# what's the big deal?

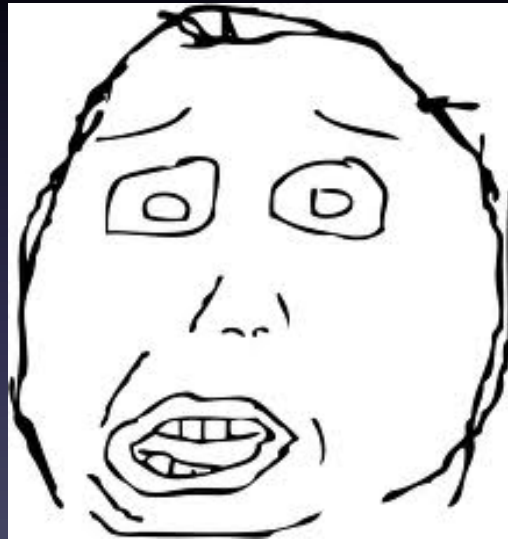
- visiting the top 50 websites will install over 3,000 tracking files on your computer
- over 80% of websites use one or more tracking tools
- online advertising is a \$50 billion business
- from the perspective of hundreds of ad & data collection companies, You Are The Product, waiting to be sold to advertisers

# still not concerned?

- data collected through your browsing can determine whether you can obtain a job, credit or insurance
- your information can be stored, analyzed, indexed and sold as a commodity to data brokers who in turn might sell it to advertisers, employers, health insurers or credit rating agencies
- online data is merged with offline data and sold
- websites vary prices and deals based on users' information

# browser thoughts

can't I just use incognito mode?



short answer: NO

# browser solutions

- epic browser
  - [www.epicbrowser.com](http://www.epicbrowser.com)
- use Tor whenever you browse (computer and android devices)
  - [www.torproject.org](http://www.torproject.org)
- use TAILS when on public computers
  - [tails.boum.org](http://tails.boum.org)

# remember

- your data belongs to you, don't compromise yourself
- only share as appropriate
- don't get taken advantage of by sharing too much data with too many people and companies



# other tidbits

- stay curious, keep your mind open
  - learning is a lifelong occupation, chase your interests
  - take the time to understand your rights
  - participate in the process by which your rights are regulated
- there is more internet than you may realize
  - anonymous sites abound, and are only available to view by anonymous browsers (Tor, I'm looking at you)

# Q&A / demo?

