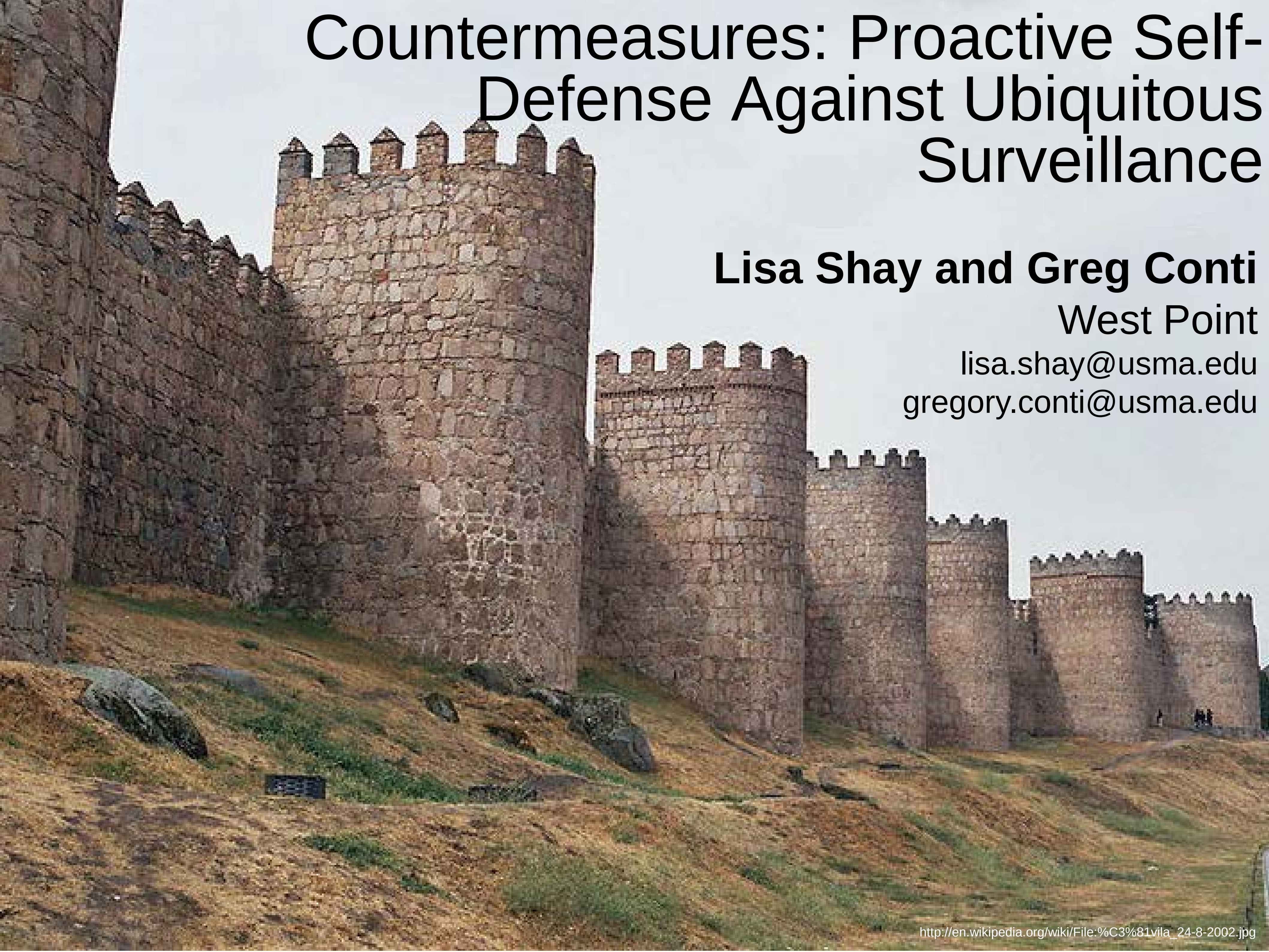
Countermeasures: Proactive Self-Defense Against Ubiquitous Surveillance

Lisa Shay and Greg Conti

West Point

lisa.shay@usma.edu

gregory.conti@usma.edu



http://en.wikipedia.org/wiki/File:%C3%81vila_24-8-2002.jpg

Disclaimers

The views in this talk are the authors’ and don’t reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.

Context matters. Some of these countermeasures are likely illegal in certain (or all) circumstances. If you have questions in this regard, consult a lawyer. We are not lawyers.

All characters and events in this show – even those based on real people – are entirely fictional. All celebrity voices are impersonated... poorly. The following program contains coarse language and due to its content it should not be viewed by anyone.

Takeaways

- Networked surveillance systems threaten our privacy and our free way of life
- Individuals can and should protect themselves
- This community has the knowledge and status to deflect the trajectory of our surveilled future

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

- Sun Tzu

http://en.wikipedia.org/wiki/File:Enchoen27n3200.jpg

Current Trends

Instrumented People

“Government of India Plans to Track Mobile Phone Users”

“World's Biggest Biometric ID Scheme Forges Ahead”
(1.2B People)

http://www.bbc.co.uk/news/world-asia-india-16979875
http://commons.wikimedia.org/wiki/File:Delhi_airport_departure_terminal_1A%281%29.JPG
http://www.indianexpress.com/news/soon-govt-will-keep-track-of-where-every-mobile-phone-user-is/912681/

Instrumented Homes

TV's that watch you.

http://www.technologyreview.com/web/38383/

http://hdguru.com/is-your-new-hdtv-watching-you/7643/

http://yro.slashdot.org/story/12/03/31/2027225/samsung-says-their-tvs-arent-really-spying-on-you

Instrumented Communities

$1 Billion Scientific “Ghost Town”

http://www.foxnews.com/scitech/2012/05/12/scientists-plan-1b-ghost-town/

New Applications

Emperor Penguins Counted from Space

http://www.bbc.co.uk/news/science-environment-17692025

New Applications

Police Use of Surveillance Drones

http://thawkmav.com/
http://www.wsvn.com/news/articles/local/21003198189967/

New Power Sources

Robojelly – Powered by Hydrogen and Oxygen in Water

Nuclear Powered Drone Research - Flight time from “days to months”

http://en.wikipedia.org/wiki/File:MQ-9_Reaper_in_flight_%282007%29.jpg
http://www.guardian.co.uk/world/2012/apr/02/us-plans-nuclear-drones
http://www.washingtontimes.com/news/2012/apr/4/scientists-build-robot-jellyfish-fueled-sea-water/

Lots of Investment

Minneapolis-St. Paul Airport launches $20M HD Surveillance Camera Project

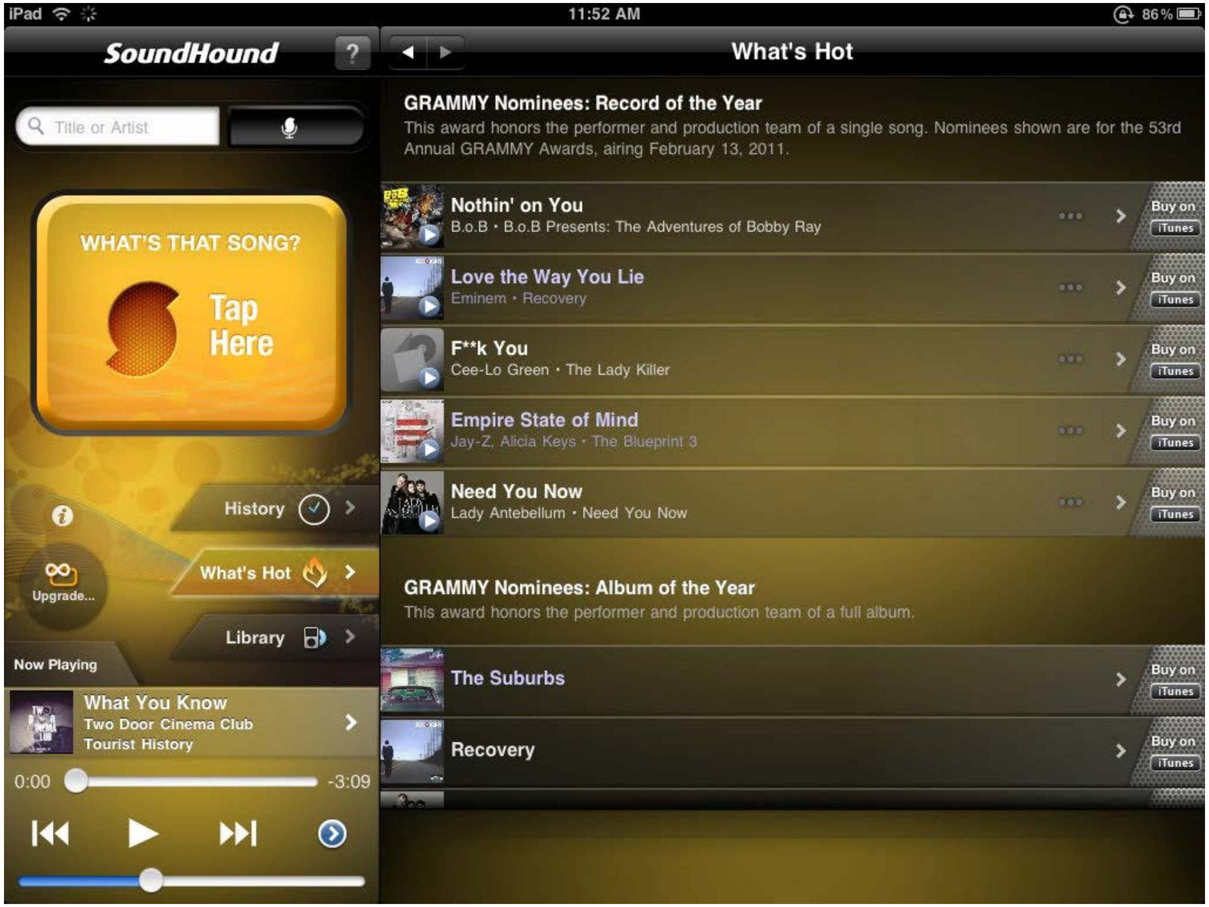
http://www.startribune.com/business/151198495.html
http://www.mspairport.com/directions/humphrey-terminal.aspx

Lots of Investment

Lower Manhattan Security Initiative

http://www.wired.com/dangerroom/2010/05/video-inside-new-york-spycam-hq/

Increased Capabilities



What's Hot

GRAMMY Nominees: Record of the Year

This award honors the performer and production team of a single song. Nominees shown are for the 53rd Annual GRAMMY Awards, airing February 13, 2011.

- Nothin' on You — B.o.B • B.o.B Presents: The Adventures of Bobby Ray
- Love the Way You Lie — Eminem • Recovery
- F**k You — Cee-Lo Green • The Lady Killer
- Empire State of Mind — Jay-Z, Alicia Keys • The Blueprint 3
- Need You Now — Lady Antebellum • Need You Now

GRAMMY Nominees: Album of the Year

This award honors the performer and production team of a full album.

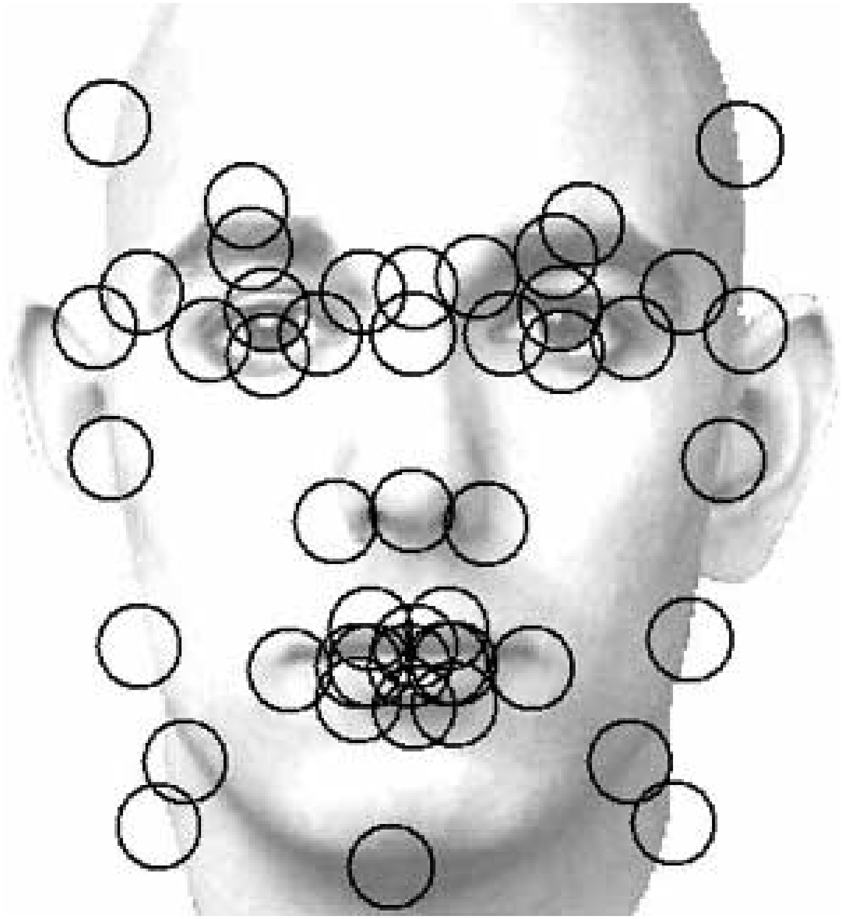
- The Suburbs
- Recovery

What You Know
Two Door Cinema Club
Tourist History

SoundHound

http://www.soundhound.com/index.php?action=s.press_release&pr=23

Increased Capabilities



Facial Recognition

http://www.economist.com/node/21524829

http://www.wpi.edu/News/Transformations/2002Spring/recognition.html

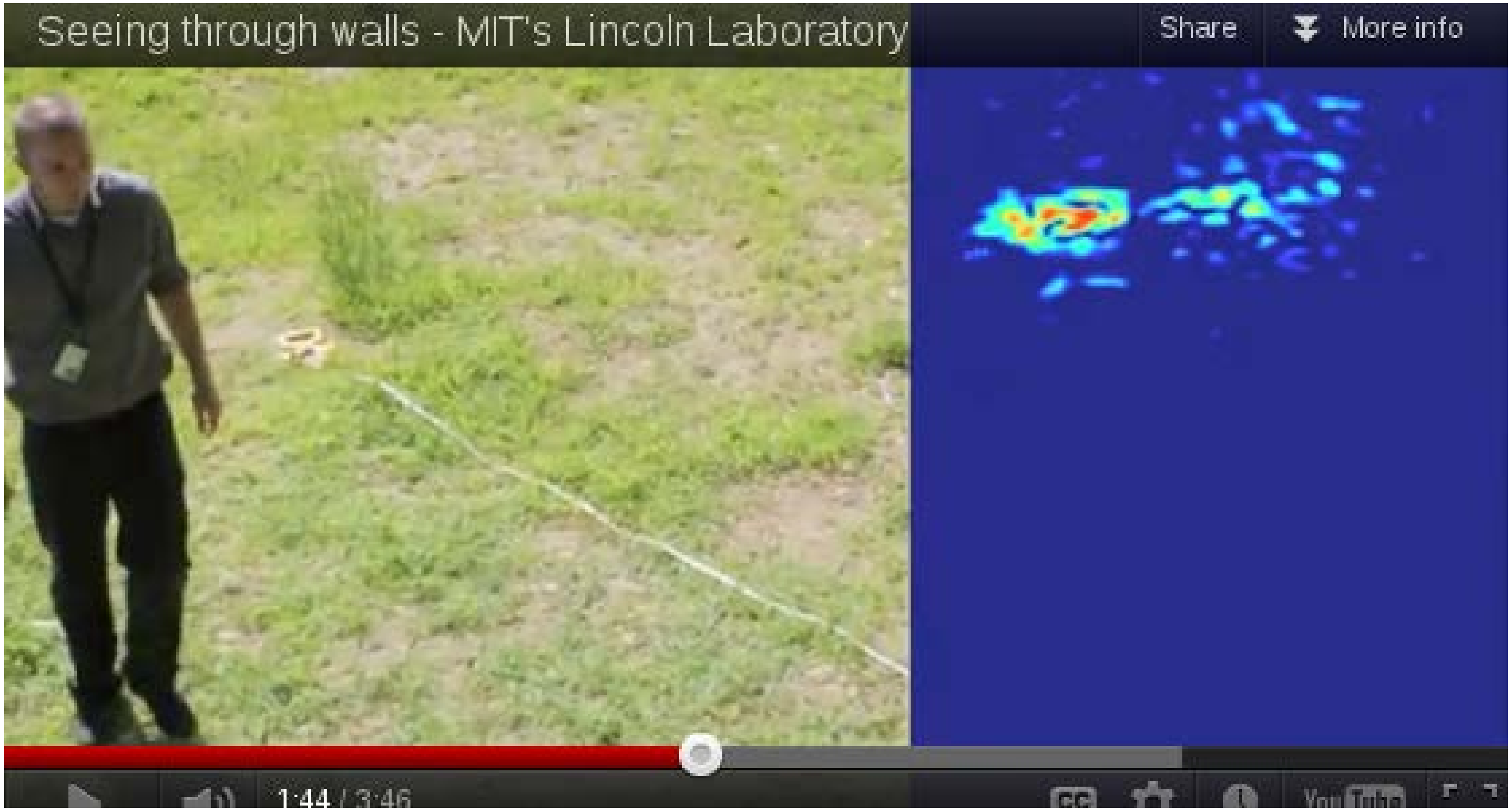
Increased Capabilities

Man-Machine Hybrid Analysis

Google Using ReCAPTCHA to Decode Street View Addresses

http://upload.wikimedia.org/wikipedia/commons/5/58/The_wilson_front_door.JPG
http://techcrunch.com/2012/03/29/google-now-using-recaptcha-to-decode-street-view-addresses/
http://tech.slashdot.org/story/12/03/29/2055228/google-using-recaptcha-to-decode-street-addresses

Increased Capabilities



MIT Lincoln Lab Technology Provides Real-Time Video Through Solid Walls

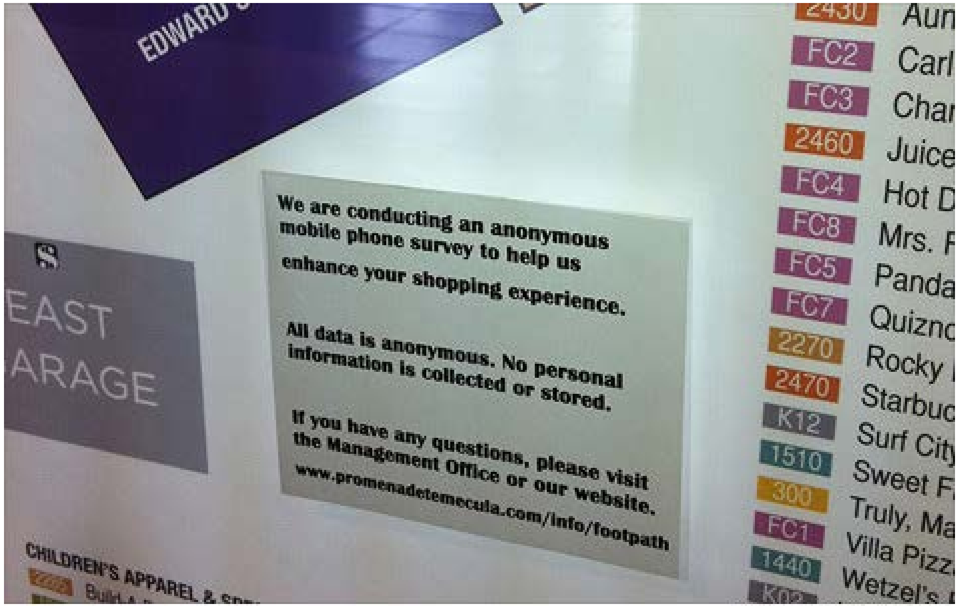
http://web.mit.edu/newsoffice/2011/ll-seeing-through-walls-1018.html

New Incentives

GPS used for Driving Insurance “Discounts”

http://en.wikipedia.org/wiki/File:KyotoTaxiRide.jpg
http://www.inautonews.com/wp-content/plugins/yet-another-photoblog/ cache/tomtom_pro_3100_insurance.65yvmqcnmwsgooooc4sswck8s.a5fuq7lrqzkgc0ccw4ss08gso.th.jpeg

Old Reasons



We are conducting an anonymous mobile phone survey to help us enhance your shopping experience.

All data is anonymous. No personal information is collected or stored.

If you have any questions, please visit the Management Office or our website.
www.promenadetemecula.com/info/footpath

COURTESY: FOREST CITY

"We are conducting an anonymous mobile phone survey to help us enhance your shopping experience."

Malls Track Shoppers' Cell Phones

http://money.cnn.com/2011/11/22/technology/malls_track_cell_phones_black_friday/index.htm

Coercive Disclosure of Identity

Google+ Real-Name Policy

http://www.zdnet.com/blog/networking/google-revises-google-real-name-management-policy/1278

Same System Vulnerabilities

See...

Tom Cross, “Exploiting Lawful Intercept to Wiretap the Internet” Black Hat DC 2010

Zeljka Zorz, “Most CCTV Systems are Easily Accessible to Attackers” Help Net Security

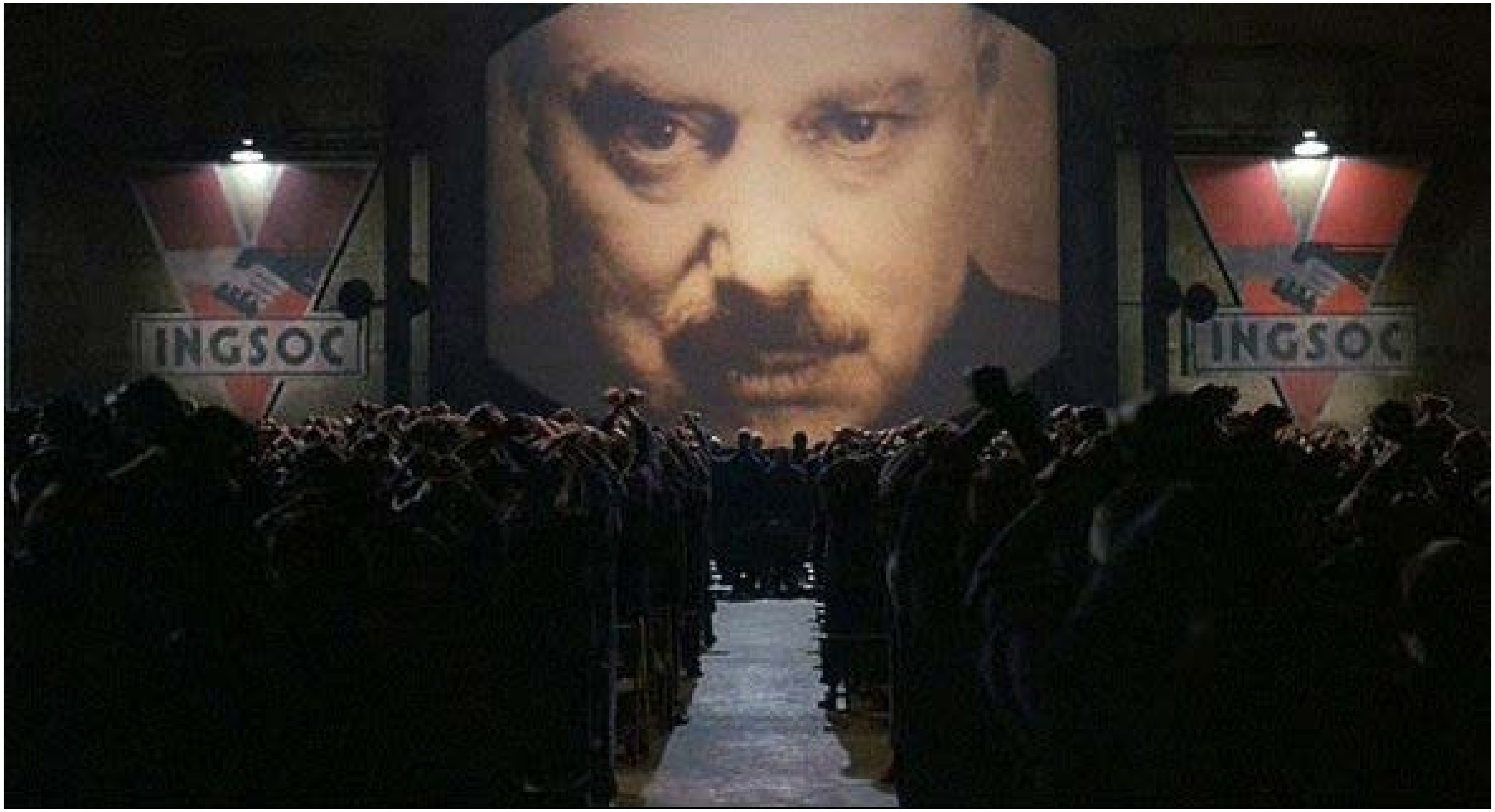
http://commons.wikimedia.org/wiki/File:Pinscher_puppy.jpg

Lots of “Blue-Sky Ideas”

US Postal Trucks as Fleet of Sensor Platforms

http://lynnjenkins.house.gov//images/user_images/Post%20Office.jpg
http://science.slashdot.org/story/10/12/19/2216202/a-blue-sky-idea-for-the-usps-postal-trucks-as-sensors

The Potential for Misuse is High...



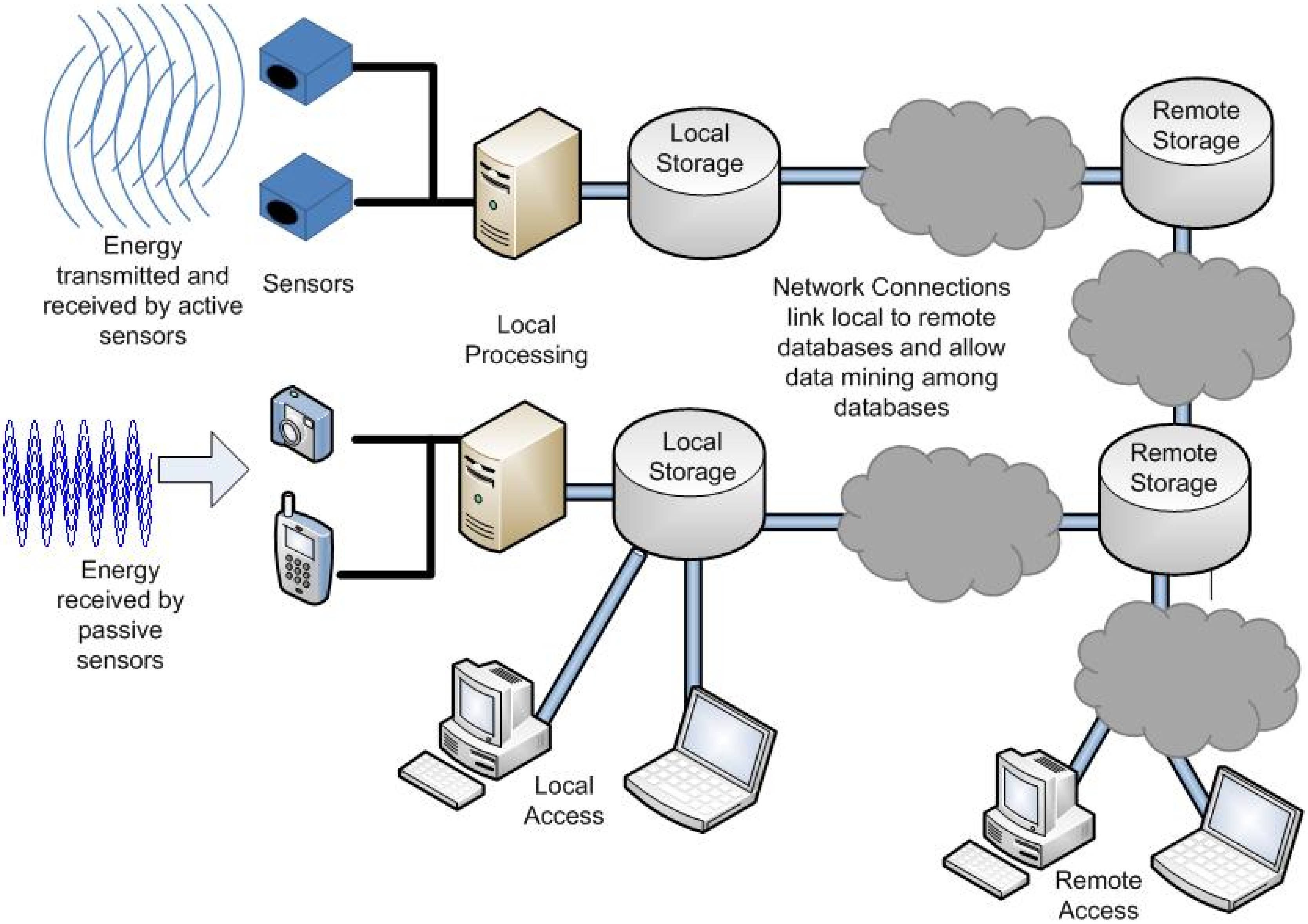
http://gadgetcrave.frsucrave.netdna-cdn.com/wp-content/uploads/2011/04/1984-movie

We'll Leave Online Surveillance for Another Talk...

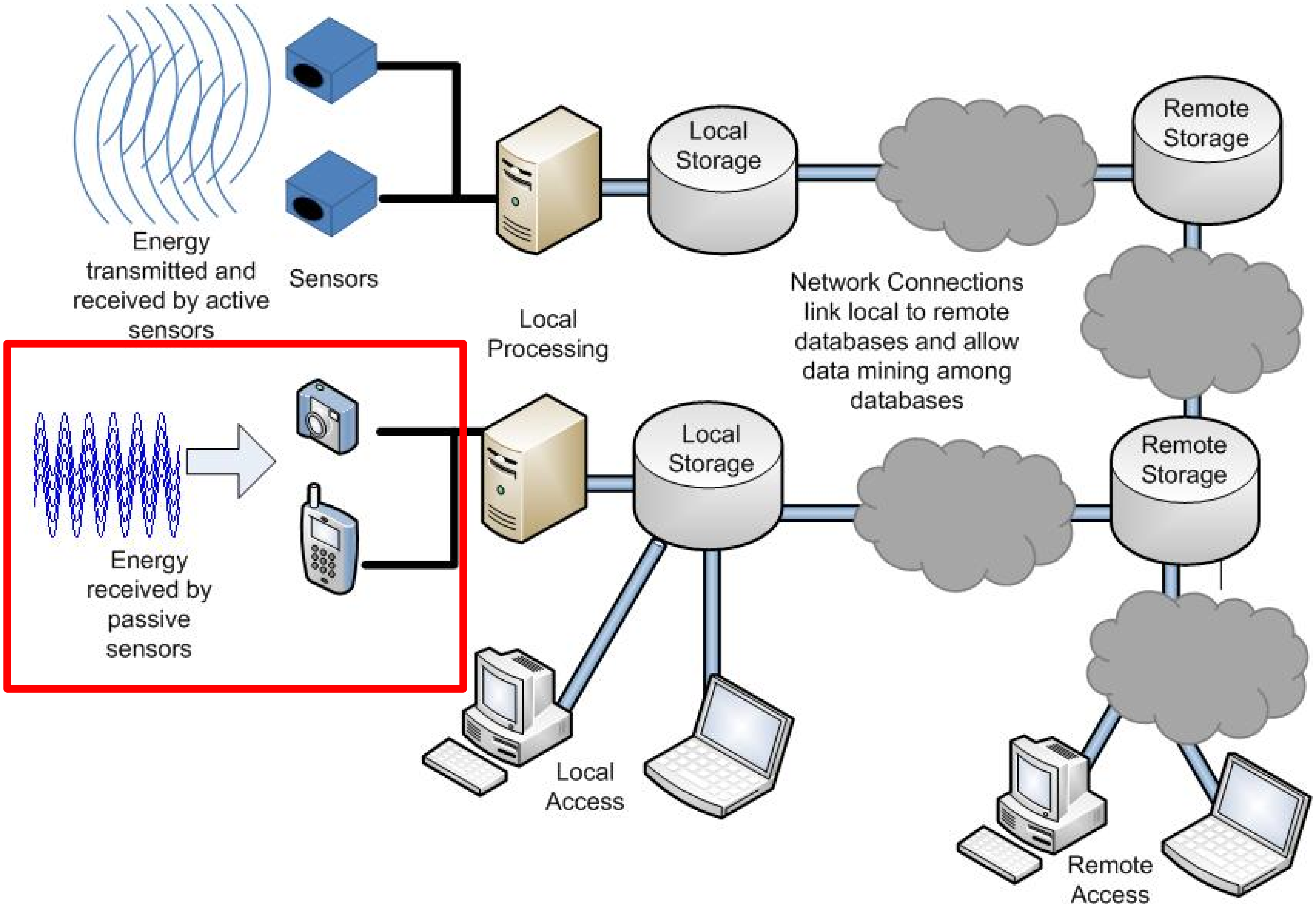
http://corcodilos.com/blog/wp-content/uploads/2011/11/big-brother.jpg

Deconstructing a Surveillance System

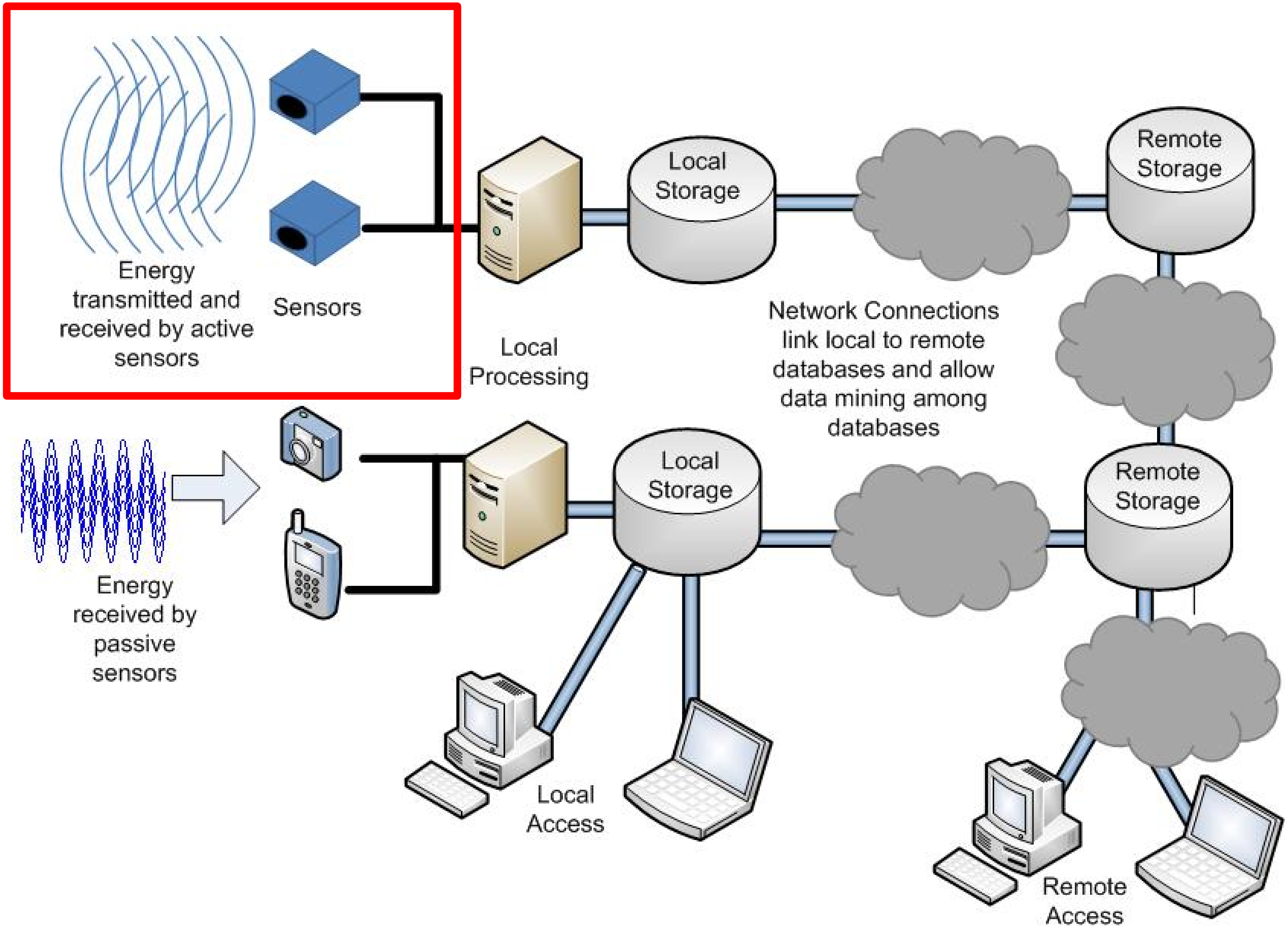
Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Local Storage
Remote Storage
Energy received by passive sensors
Local Access
Remote Access

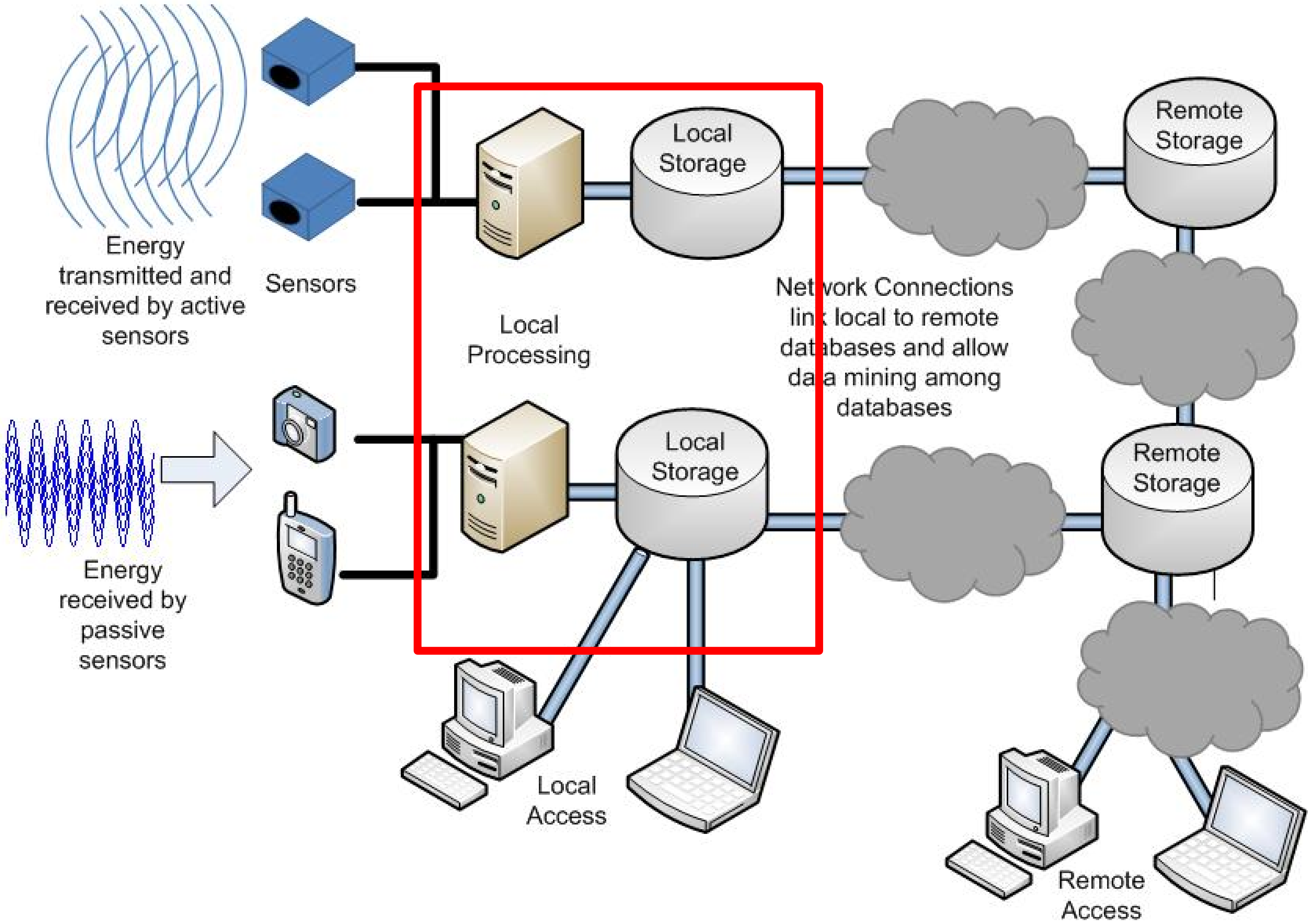
Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Local Storage
Remote Storage
Energy received by passive sensors
Local Access
Remote Access

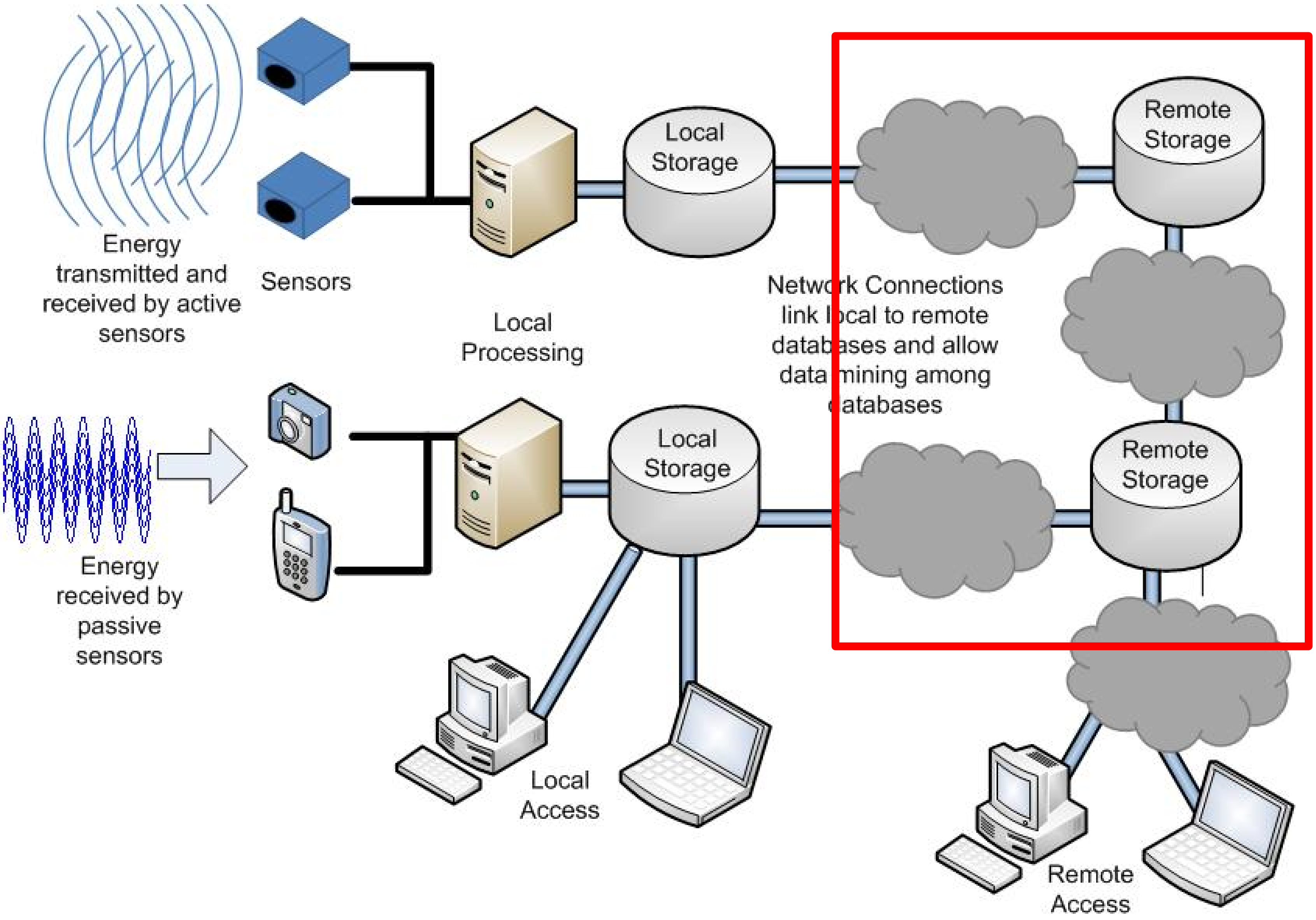
Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Local Storage
Remote Storage
Energy received by passive sensors
Local Access
Remote Access

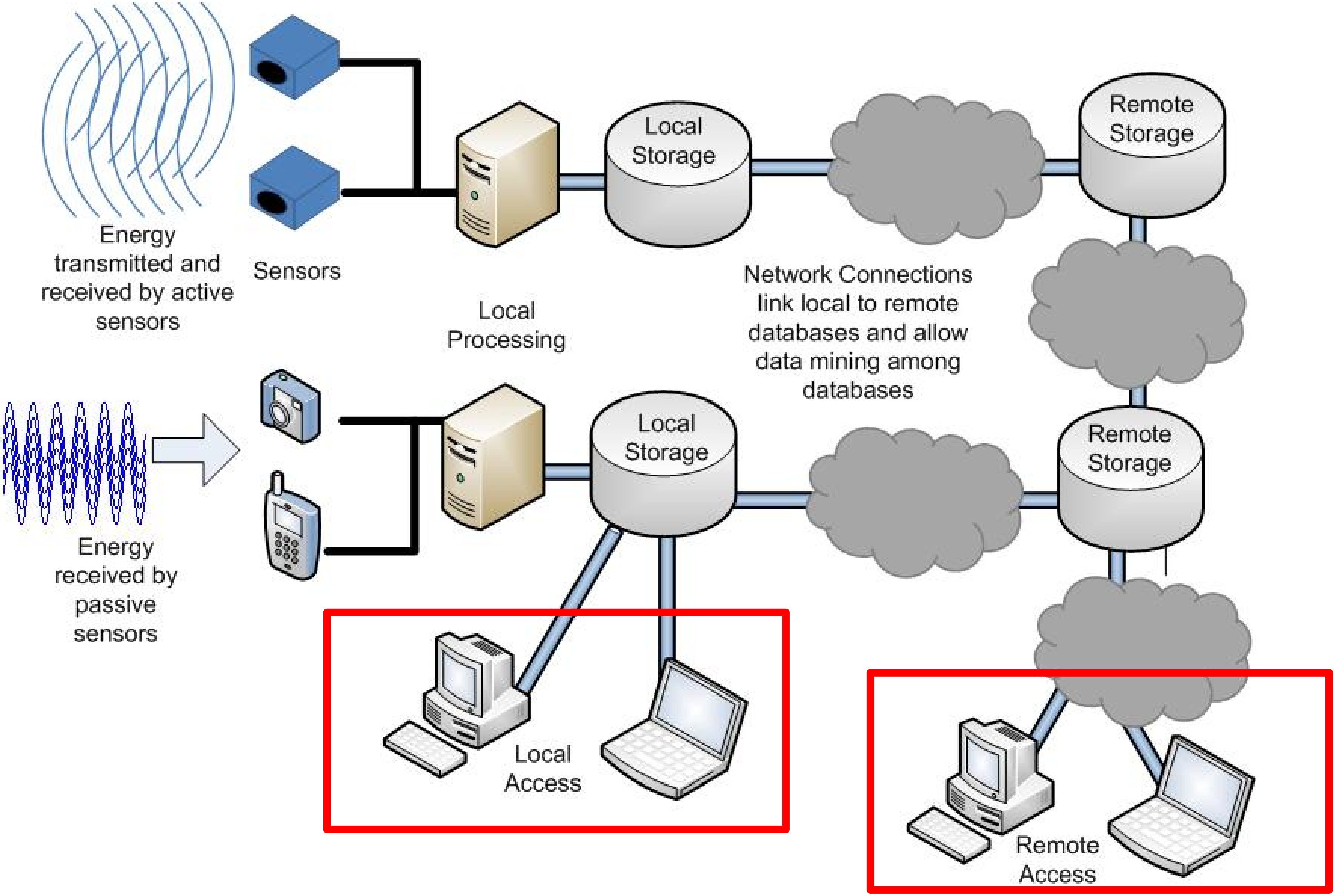
Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Energy received by passive sensors
Local Processing
Local Storage
Local Storage
Network Connections link local to remote databases and allow data mining among databases
Remote Storage
Remote Storage
Local Access
Remote Access

Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Network Connections link local to remote databases and allow data mining among databases
Remote Storage
Remote Storage
Local Storage
Energy received by passive sensors
Local Access
Remote Access

Surveillance System Model


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access

Countermeasures

Understand the Sensor/System

FLASHING WHEN TIME IS EXPIRED
U S AND FOREIGN PATENTS PENDING
COVERED BY U.S. PATENTS
4,216,461 5,109,972 4,369,442
Ser.# 7-001387 REF #77300N-634 ORDER #M8485
DUNCAN 7700

- Acquire
- Understand
- Take it apart
- Spec sheets
- Range
- Power consumption
- Processing ability
- Sampling rate
- Response time
- Sensitivity
- Age
- Maintenance
- Environment
- Limitations
- Vulnerabilities

See Joe Grand, Jacob Appelbaum, and Chris Tarnovsky's Defcon 17 “Smart Parking Meter” Talk

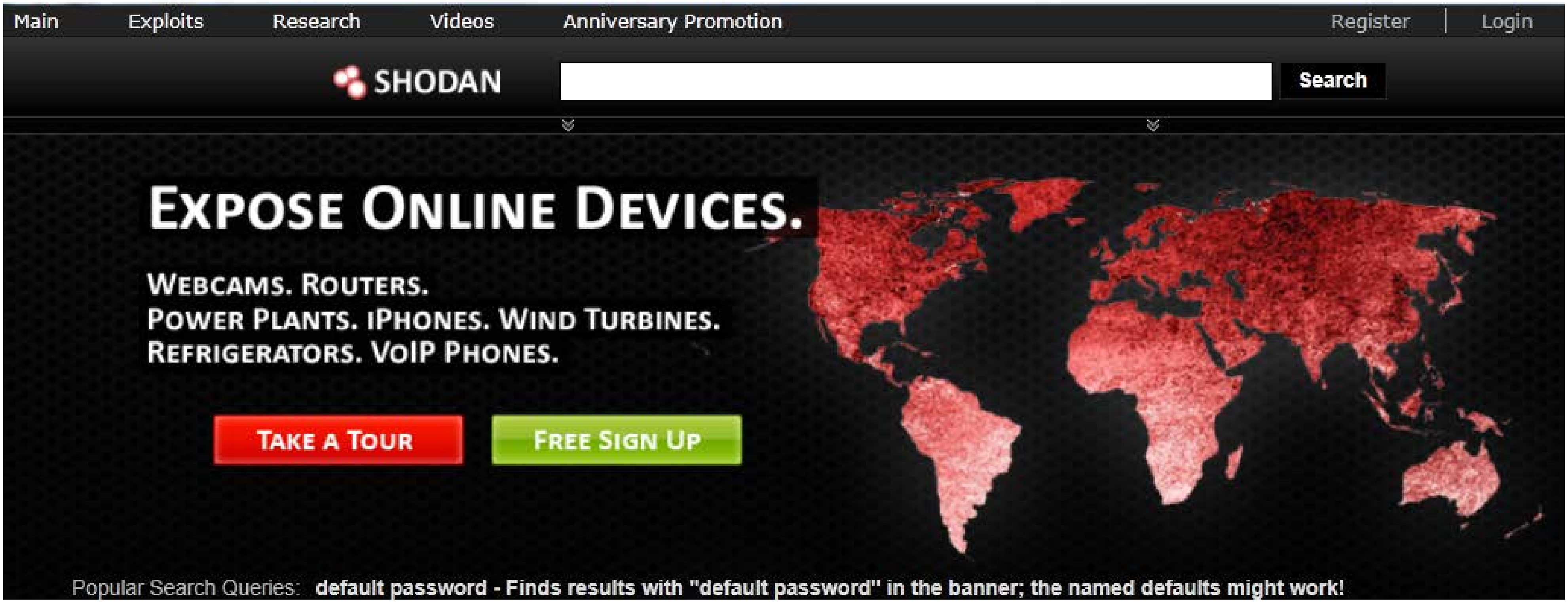
Deny, Degrade, Defeat Sensors

Detect

Car Radar Detector (Japan)

http://en.wikipedia.org/wiki/File:Car_radar_detector.jpg

Detect

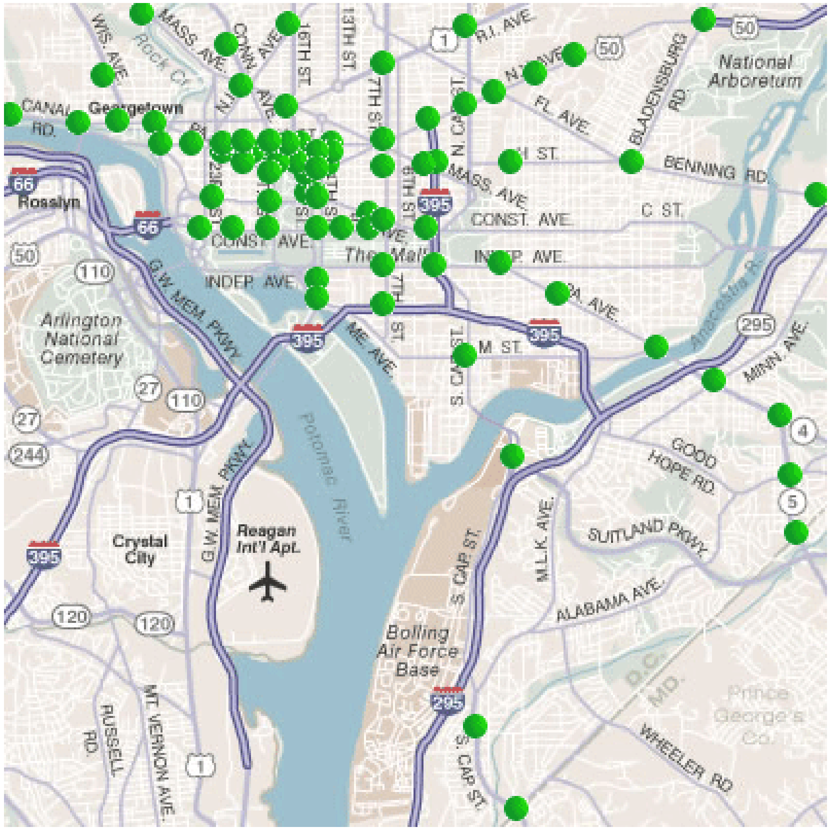


Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!

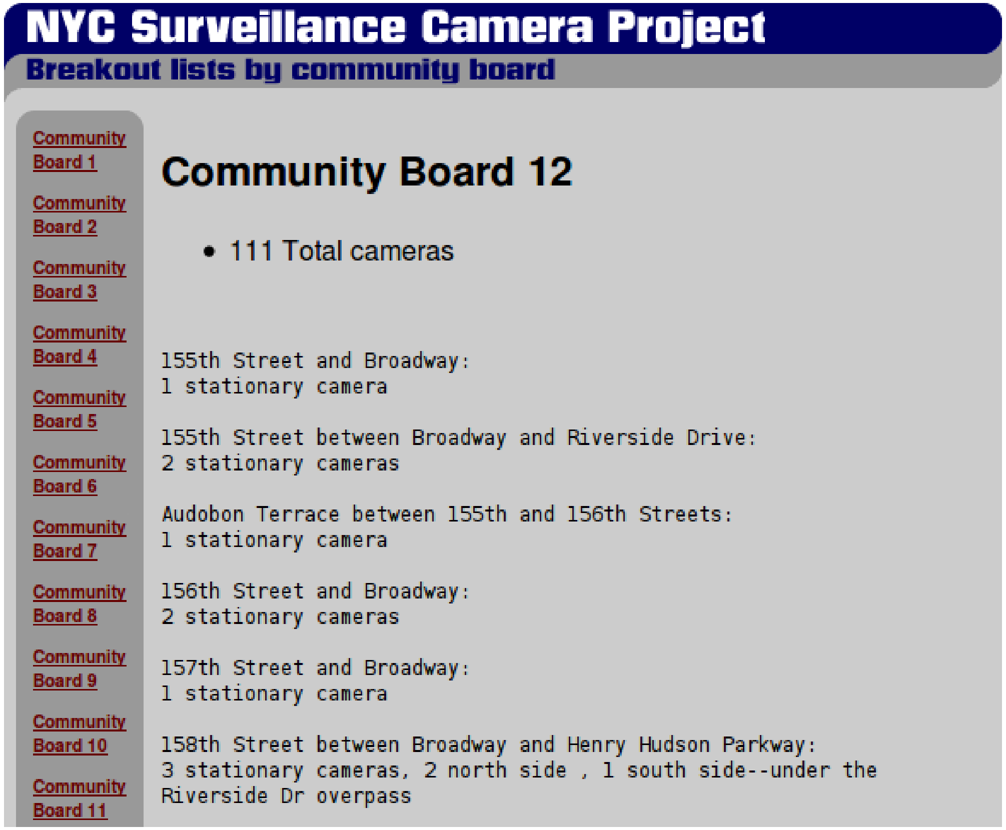
Networked Sensors may be visible online

http://www.shodanhq.com/

Monitor Location and Time of Use



Washington DC Area DDOT Traffic Camera Locations (Government Data)



NYC Surveillance Camera Project

Breakout lists by community board

Community Board 1
Community Board 2
Community Board 3
Community Board 4
Community Board 5
Community Board 6
Community Board 7
Community Board 8
Community Board 9
Community Board 10
Community Board 11

Community Board 12

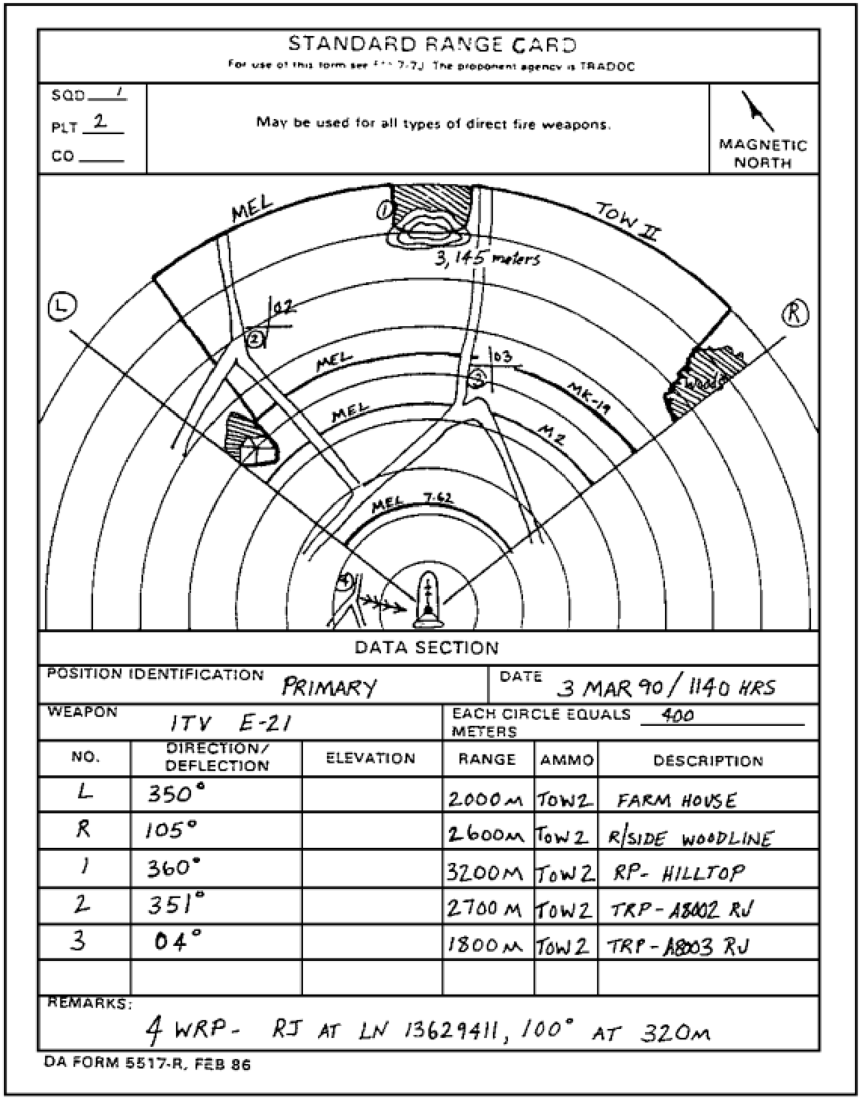
- 111 Total cameras

```
155th Street and Broadway:
1 stationary camera

155th Street between Broadway and Riverside Drive:
2 stationary cameras

Audobon Terrace between 155th and 156th Streets:
1 stationary camera

156th Street and Broadway:
2 stationary cameras

157th Street and Broadway:
1 stationary camera

158th Street between Broadway and Henry Hudson Parkway:
3 stationary cameras, 2 north side , 1 south side--under the
Riverside Dr overpass
```

NYC Surveillance Camera Project (Community Driven)

http://www.mediaeater.com/cameras/info/cb-12.html
app.ddot.dc.gov/services_dsf/traffic_cameras/map_10.asp

Understand Range and Coverage



STANDARD RANGE CARD

For use of this form see [illegible] 7-7J The proponent agency is TRADOC

SQD 1

PLT 2

CO ____

May be used for all types of direct fire weapons.

MAGNETIC NORTH

MEL
TOW II
①
3,145 meters
Ⓛ
Ⓡ
02
②
MEL
03
③
MK-19
Woods
MEL
M2
MEL
7.62
④

DATA SECTION

POSITION IDENTIFICATION PRIMARY	DATE 3 MAR 90 / 1140 HRS
WEAPON ITV E-21	EACH CIRCLE EQUALS 400 METERS

NO.	DIRECTION/ DEFLECTION	ELEVATION	RANGE	AMMO	DESCRIPTION
L	350°		2000M	TOW2	FARM HOUSE
R	105°		2600M	TOW2	R/SIDE WOODLINE
1	360°		3200M	TOW2	RP- HILLTOP
2	351°		2700M	TOW2	TRP - A8002 RJ
3	04°		1800M	TOW2	TRP - A8003 RJ

REMARKS:

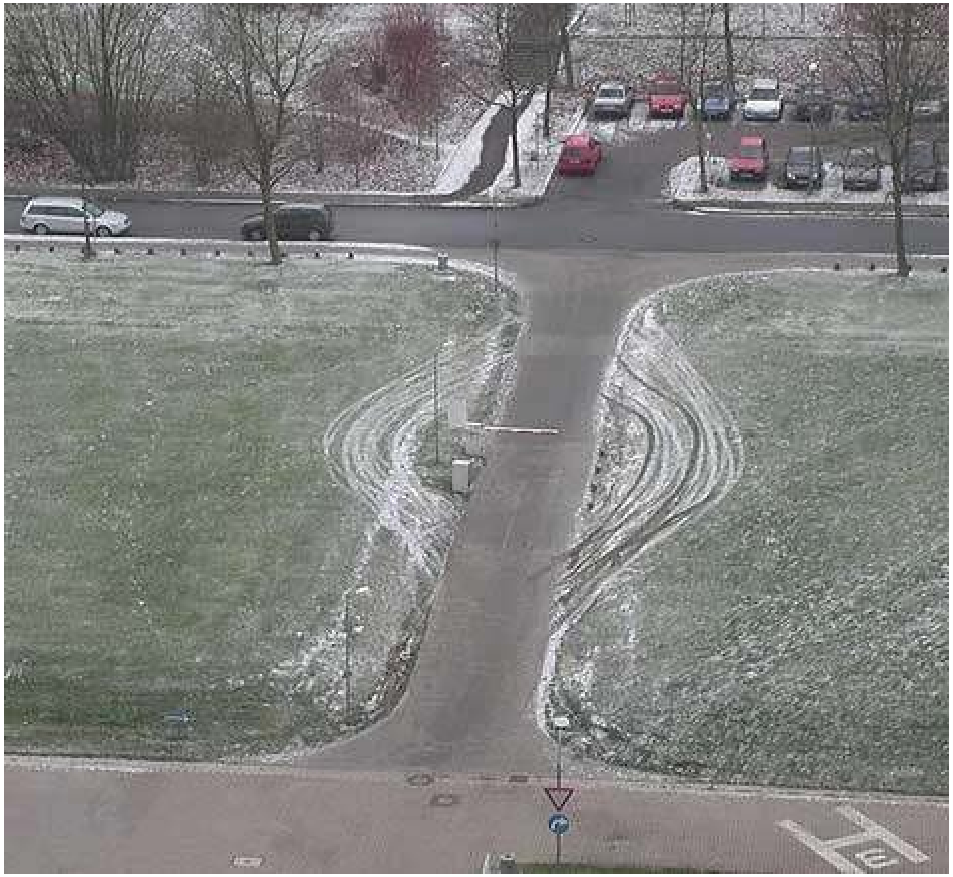
4 WRP- RJ AT LN 13629411, 100° AT 320M

DA FORM 5517-R, FEB 86

Improved TOW Vehicle Range Card

http://www.globalsecurity.org/military/library/policy/army/accp/in0542/lsn1.htm

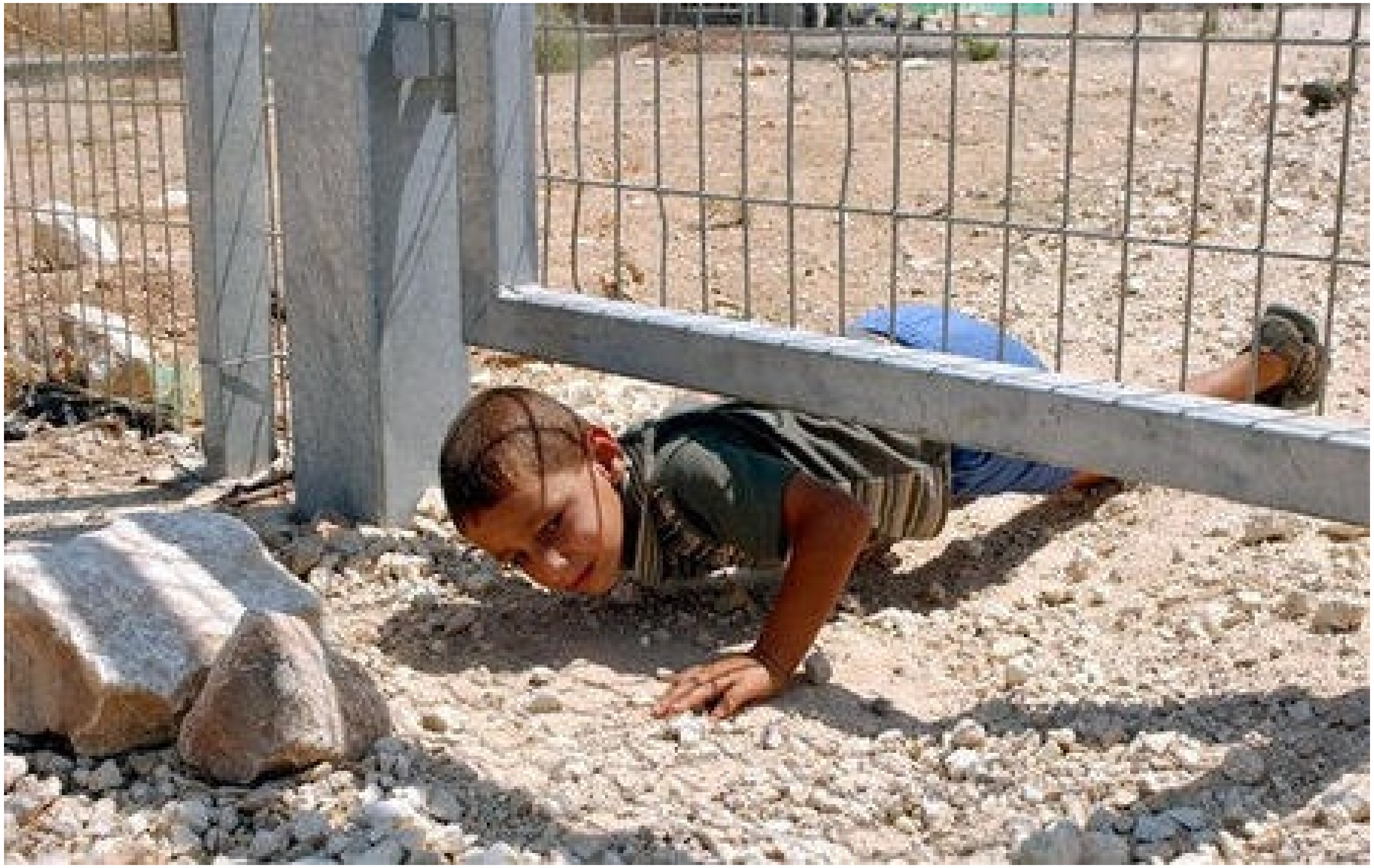
Bypass



Bypass

http://www.secmeme.com/2011/05/some-access-controls-are-easier-to.html

Bypass



http://lawrenceofcyberia.blogs.com/news/2006/12/western_news_me.html

Sampling Rate, Sensitivity

BUSTED - A heat detector can be fooled by heating the room to body temperature.

CONFIRMED - A heat detector can be fooled by wearing a highly insulated fire proximity suit.

CONFIRMED - A heat detector can be fooled by placing glass between the intruder and the sensor.

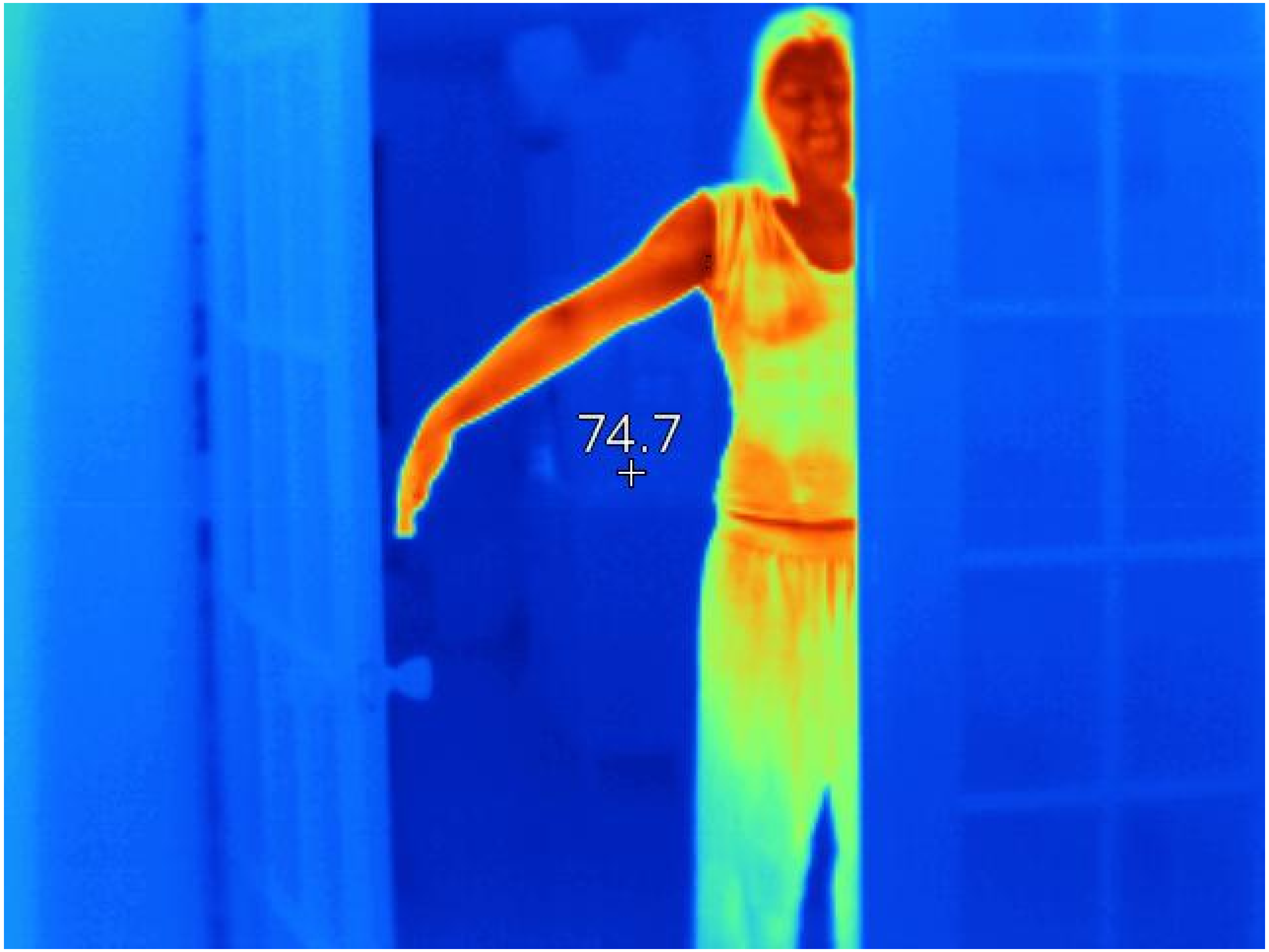
BUSTED - An ultrasonic motion detector can be fooled by wearing thick-padded clothing.

CONFIRMED - An ultrasonic motion detector can be fooled by holding a bedsheet in front of you.

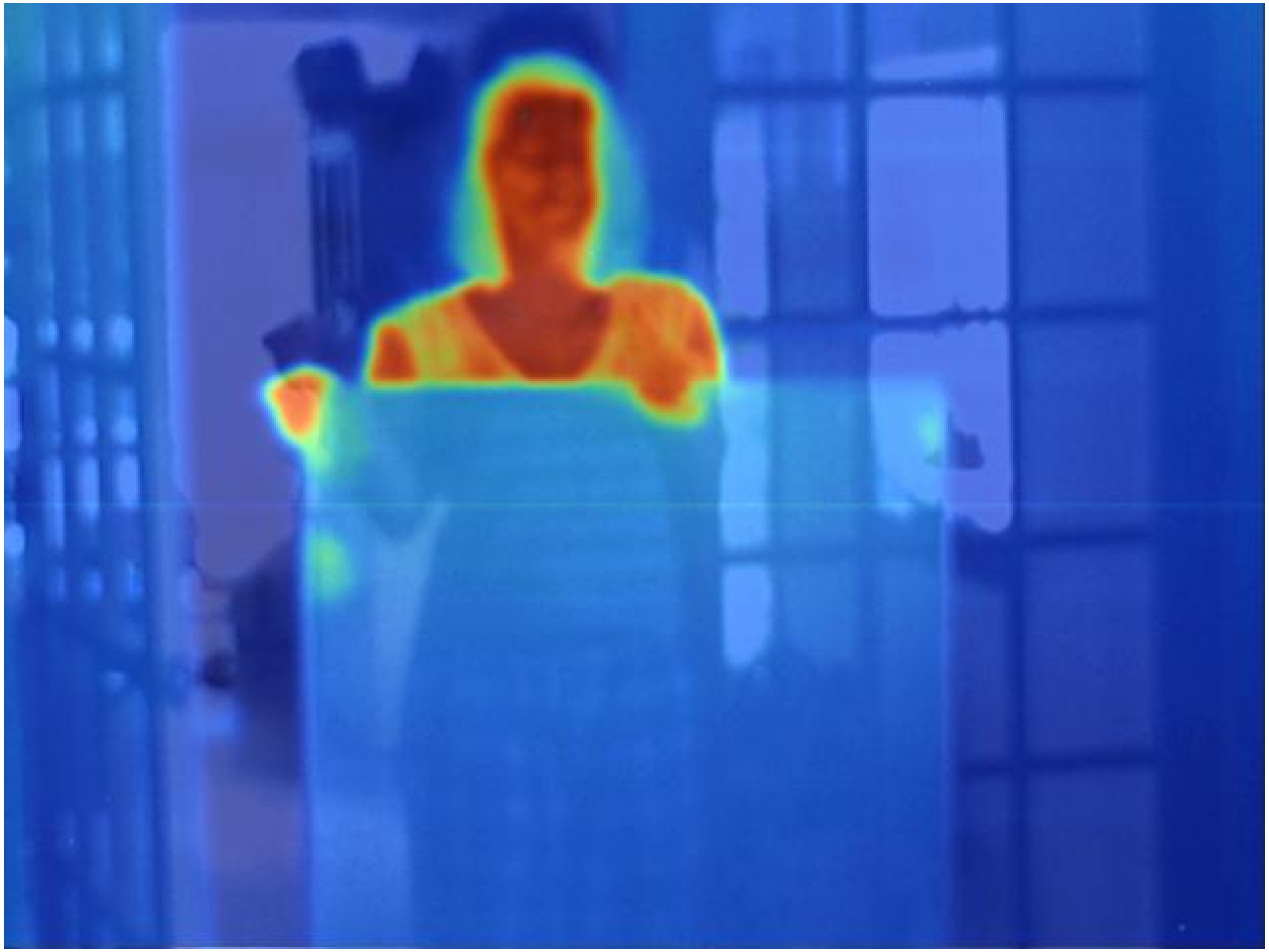
CONFIRMED - An ultrasonic motion detector can be fooled by moving extremely slowly.

See http://mythbustersresults.com/episode59

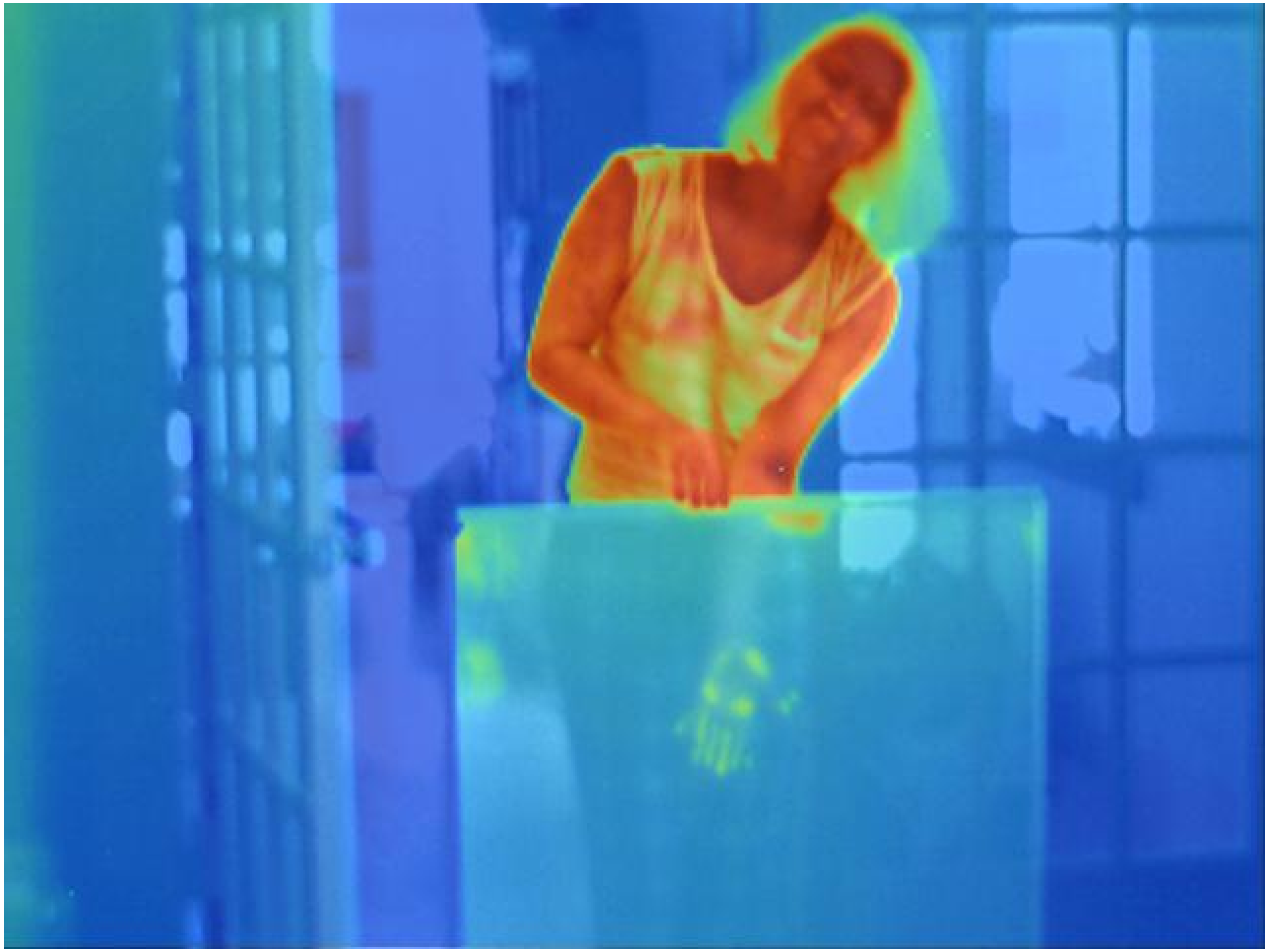
Glass Blocks IR



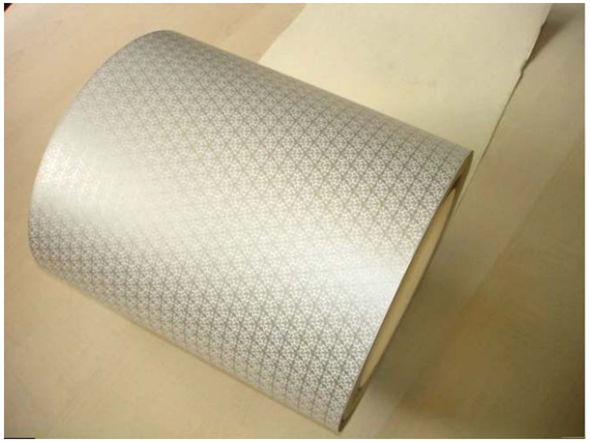
As Does Acrylic



But Be Careful How You Hold It



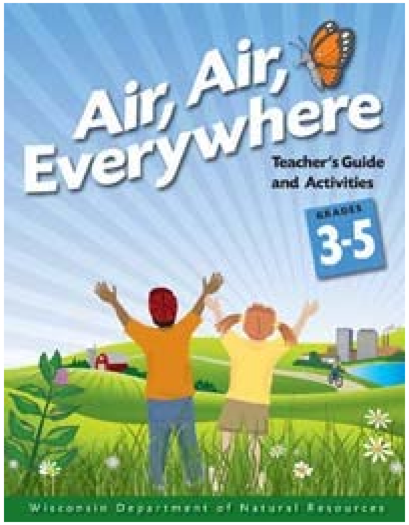
Shielding



Wi-Fi Shielding Wallpaper

RFID Blocking Wallet

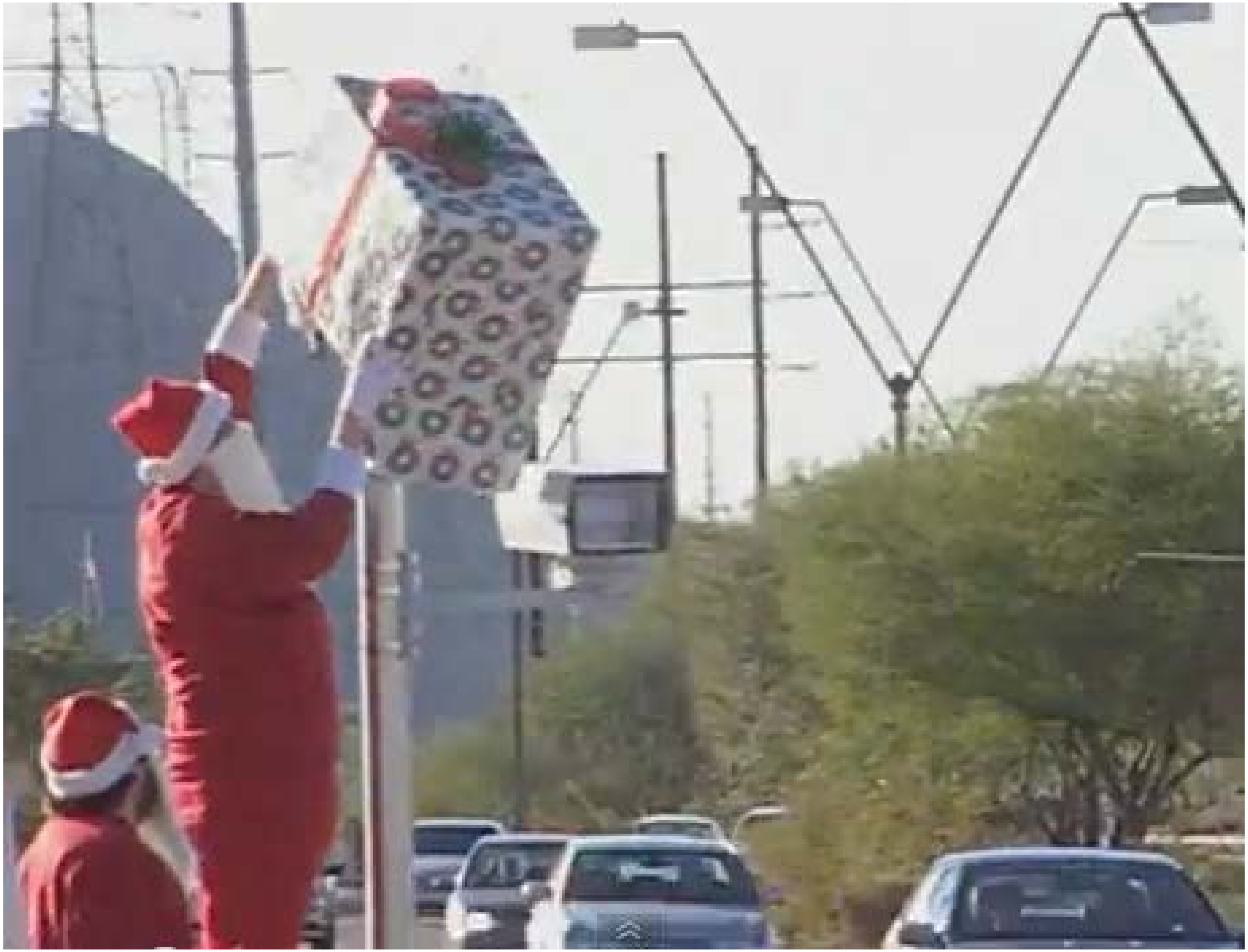
Laptop Compubody Sock


Air, Air, Everywhere
Teacher's Guide and Activities
GRADES
3-5
Wisconsin Department of Natural Resources

Stand-off Distance / Air Gap

http://www.thinkgeek.com/gadgets/security/8cdd/
http://sternlab.org/2008/04/body-technology-interfaces/
http://www.wired.com/design/2012/05/identity-protection-wallpaper/

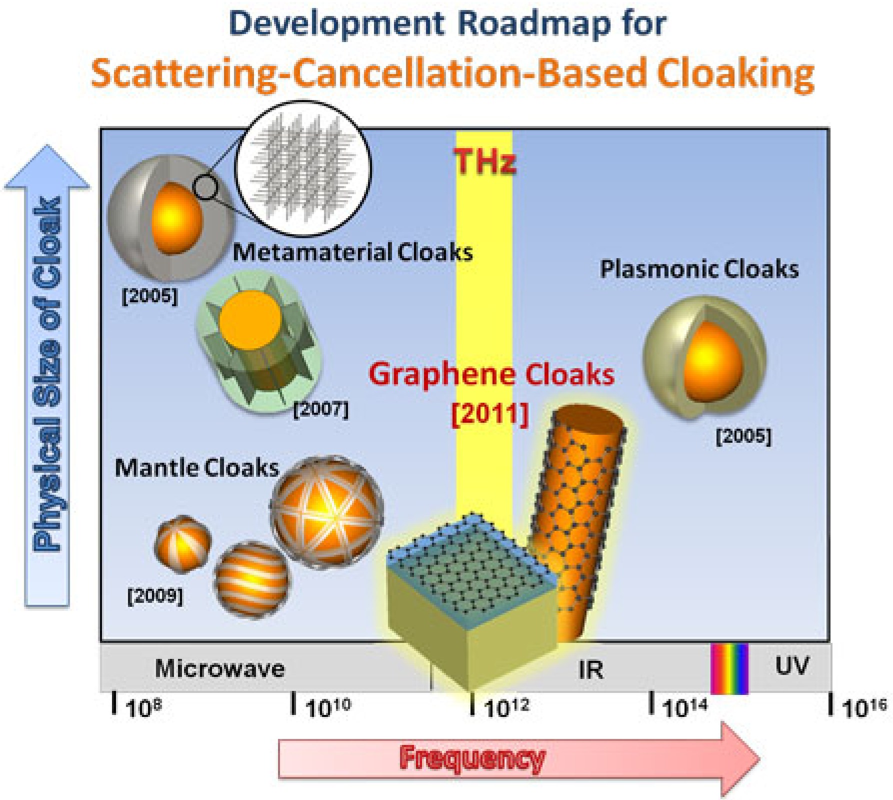
Shielding



Santa's Helpers Disable Naughty Cameras in Tempe

http://www.youtube.com/watch?v=T43LtGNFLPw

Cloaking



Graphene-based Invisibility Cloak

http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/graphene-enables-invisibility-cloak

Chaffing

Navy Wants Ultraviolet Cloaking Device for Jet Fighters

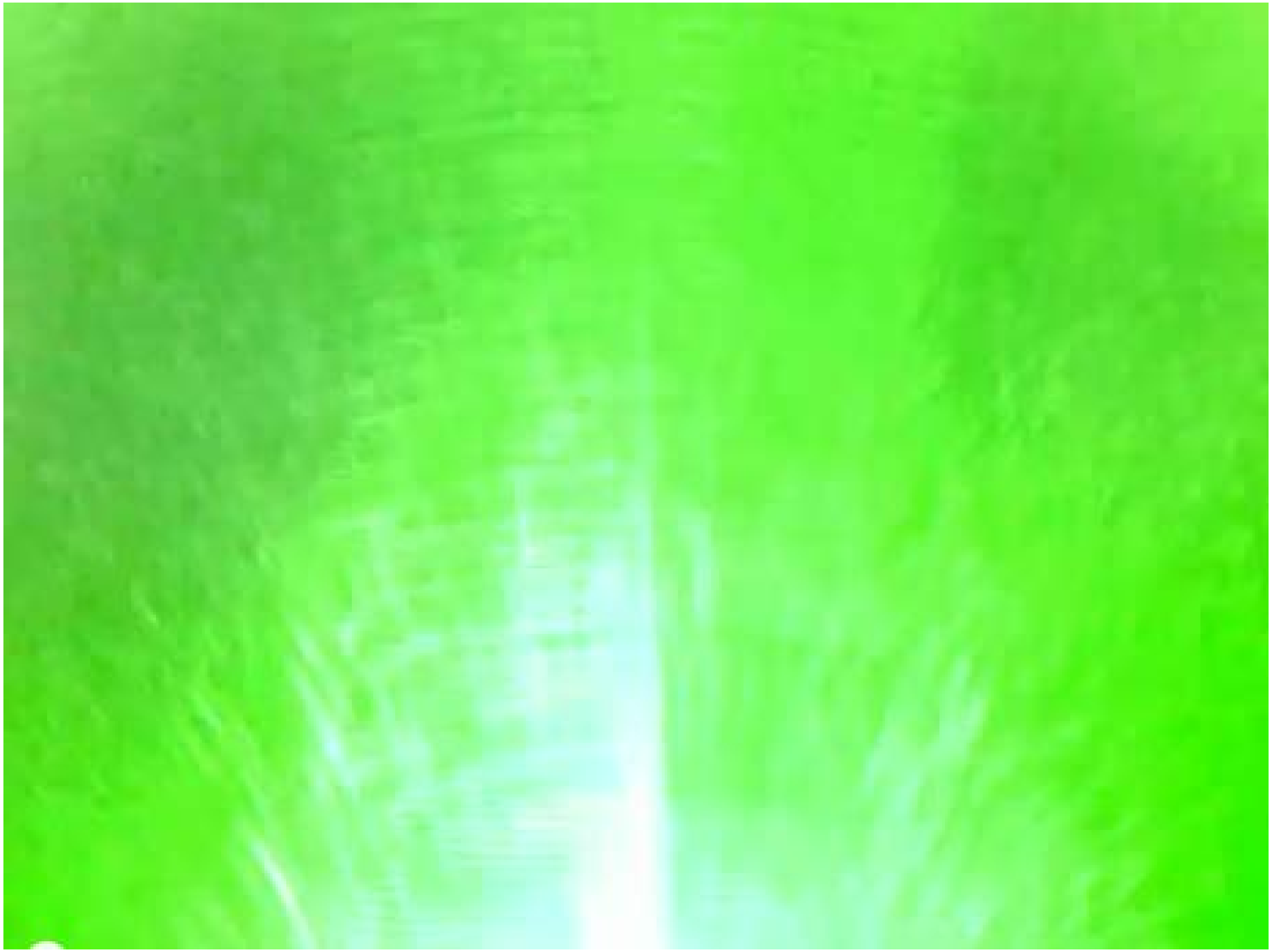
http://www.wired.com/dangerroom/2012/05/navy-uv-cloak/

Absorption

Radar Absorbing Materials

http://oceanexplorer.noaa.gov/explorations/05deepscope/logs/aug28/media/galv_boats_on_radar.html

Jam



Green Laser Pointer in Webcam

http://www.youtube.com/watch?v=cay382lod70

Destroy

Microwave Oven HERF Gun

http://www.youtube.com/watch?v=20PtFoyu0ZI

Disable

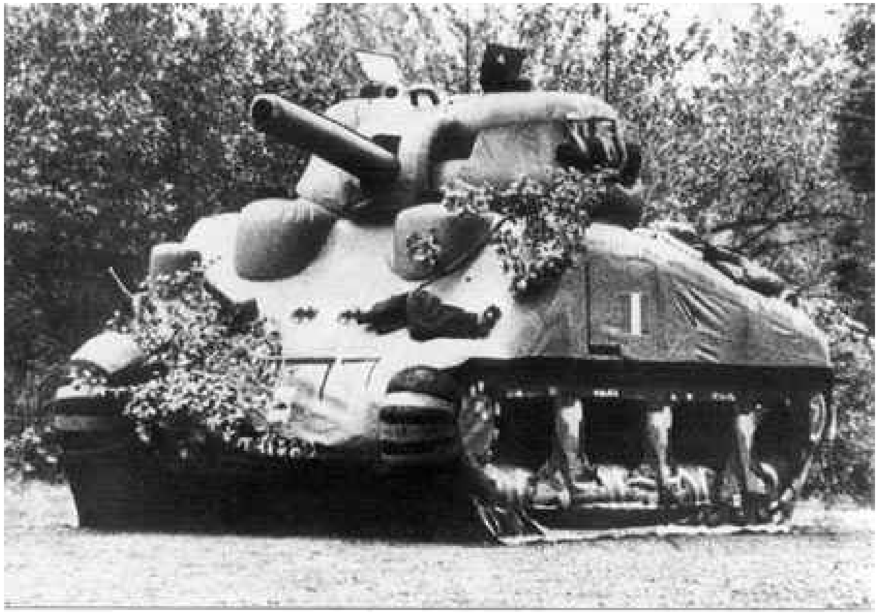
Black Tape

Microphone Plugs

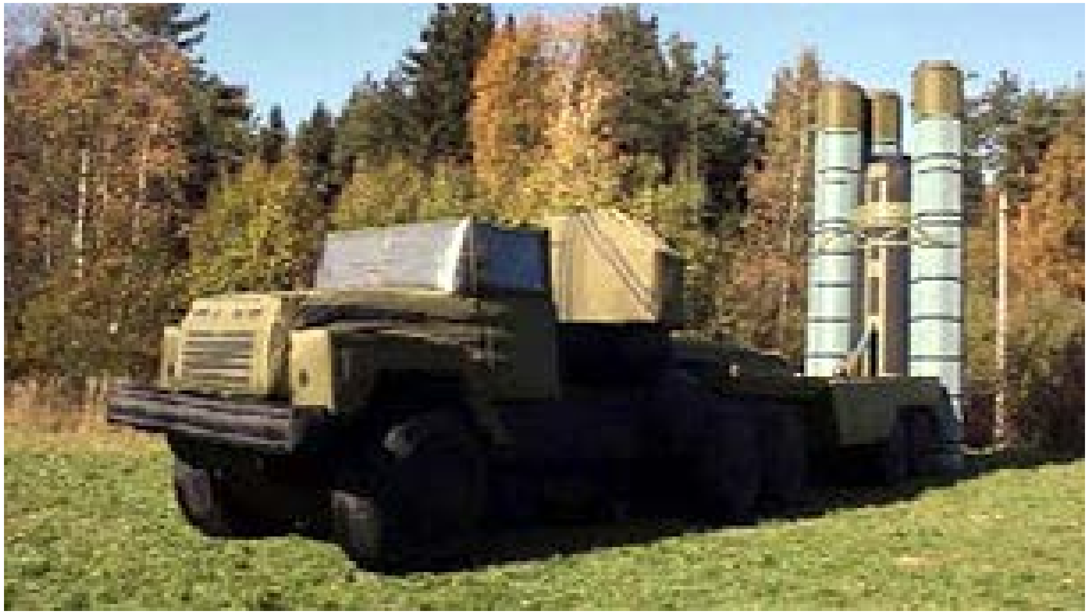
http://commons.wikimedia.org/wiki/File:Electrical-tape_black.jpg
http://www.mouser.com/ProductDetail/Neutrik/NYS231/?qs=JfNPhaIww3L40DejsZrW45j6vm7w9WEkL8akcb15MZ8%3d

Deny, Degrade, Defeat Processing

Spoofing



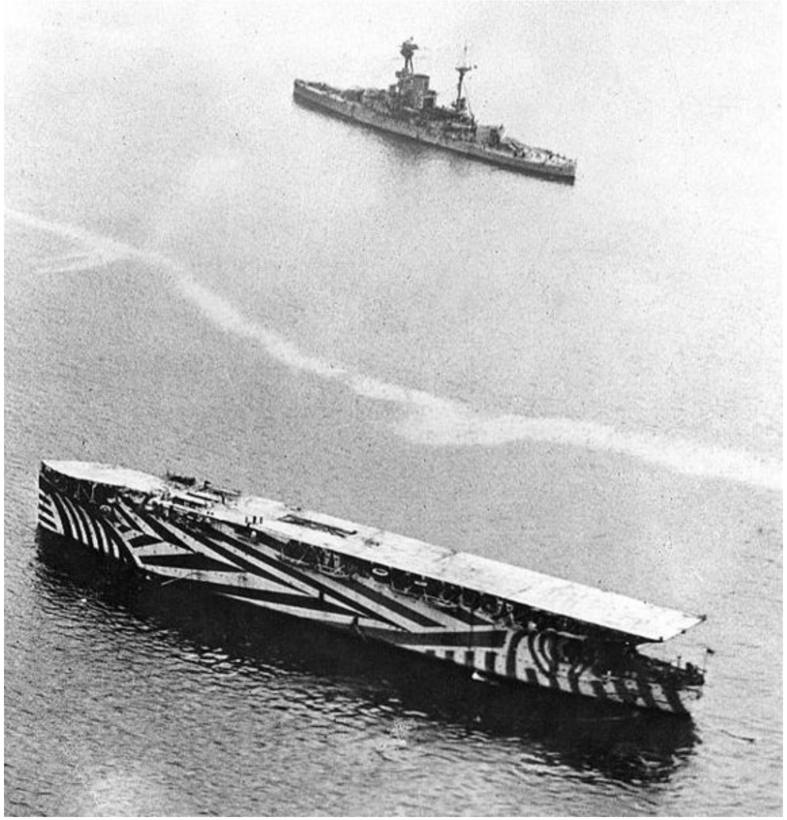
WWII Operation Bodyguard



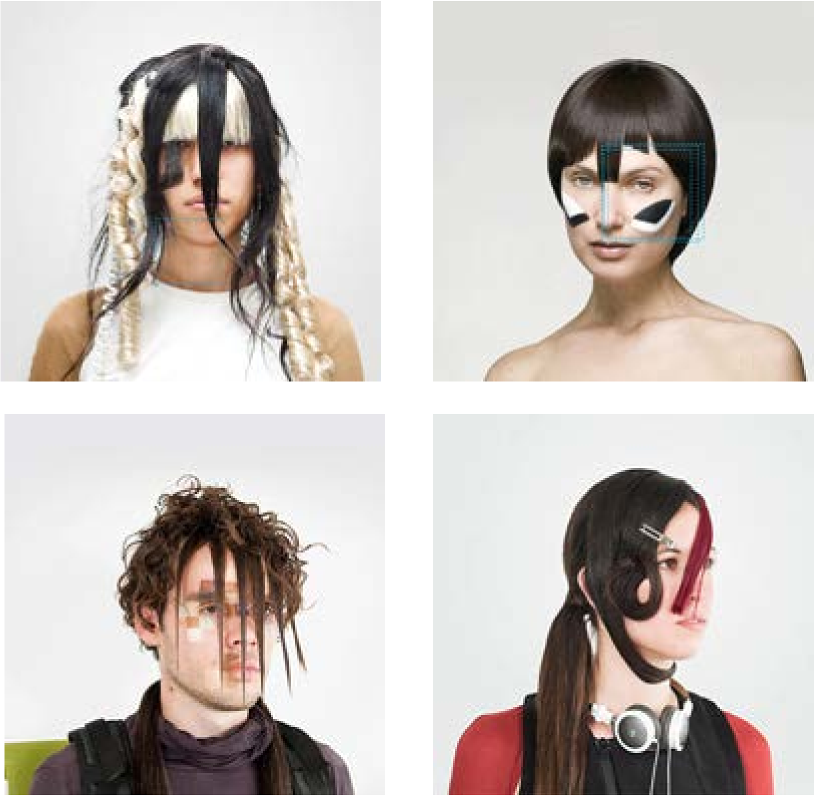
~2010 Russian Inflatable Weapons

http://en.wikipedia.org/wiki/Operation_Bodyguard
http://www.bbc.co.uk/news/world-europe-11511886

Camouflage



HMS Argus (1917)



CV Dazzle (2012)
Camouflage for Computer Vision

See Joshua Marpet's “Facial Recognition: Facts, Fiction, and Fsck-ups” from Defcon 18 and http://cvdazzle.com/

http://en.wikipedia.org/wiki/Dazzle_camouflage

Degrade Information Quality

The Prisoner - “It's Your Funeral”

http://www.webomatica.com/wordpress/images/prisoner/prisoner_10_its_your_funeral.jpg

Overcome Processing

Go to Trial: Crash the Justice System
(See NY Times 10 March 2012 story by Michelle Alexander)

http://en.wikipedia.org/wiki/File:JMR-Memphis1.jpg

Data Collection, Retention, Storage and Lifespan

Secure Data In Transit / At Rest

Privacy Glasses

```
89 24 59 c8 cf fd 88 d1 53 b9 38 82 b3 6d 58 9a
14 00 67 68 ec 92 5a 6d 44 92 75 db 2a b3 36 2b
37 1a 44 21 96 d9 12 b6 71 b4 cf f6 45 9a a5 68
19 6c 95 f2 ae 65 61 91 3a 1b da 1d 6f 22 eb be
c3 20 cc 62 24 54 e5 53 b9 04 82 2b eb a7 d8 67
75 9b 12 b5 1f c8 b9 c2 aa 8b 79 cd 09 b2 7d a2
92 82 b3 4c c1 1f 2c 4c 9a bc 3b f2 75 e8 07 47
7e 1a fa 41 cc 41 b9 c4 e6 12 1c ce 31 67 15 cf
```

Encryption

http://www.instructables.com/id/Privacy-monitor-made-from-an-old-LCD-Monitor/

Destroy Data

Shredder (SSI)

Degausser (Japanese Platform)

See also overflow or corrupt storage and resource consumption in general...

http://www.ssiworld.com/watch/
http://www.diginfo.tv/v/12-0074-n-en.php

http://www.wired.com/gadgetlab/2012/03/will-it-shred-the-badass-pri-max-says-yes/

http://www.technologyreview.com/blog/helloworld/27853/?p1=blogs

Avoid Generating Data

Become a Neo-Luddite

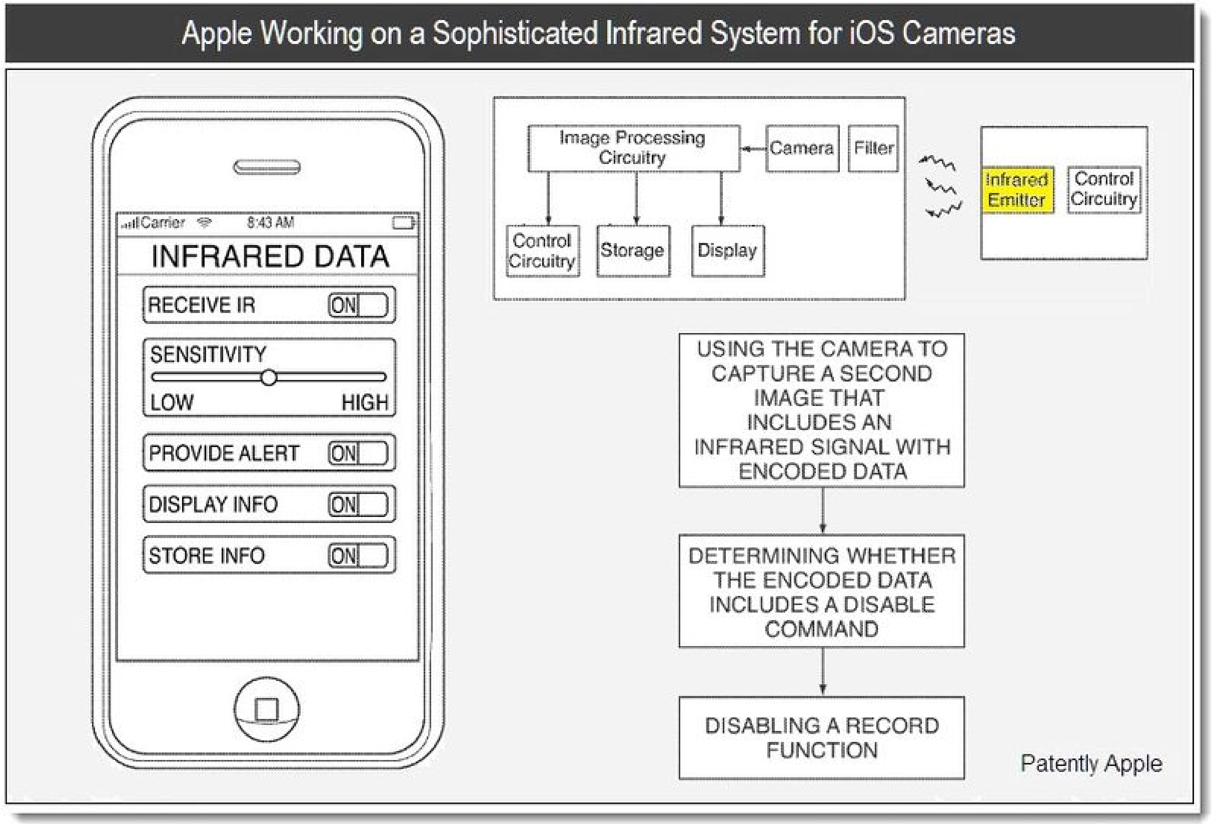
Live in the 19th Century

Live in the 20th Century

http://en.wikipedia.org/wiki/File:Luddite.jpg
http://www.fbi.gov/news/stories/2008/april/unabomber_042408
http://www.raleighnc.gov/content/SolidWaste/Images/SWS/Recycle/PhoneBook300.JPG

Communications and Command and Control

Take Control



Apple Working on a Sophisticated Infrared System for iOS Cameras

USING THE CAMERA TO CAPTURE A SECOND IMAGE THAT INCLUDES AN INFRARED SIGNAL WITH ENCODED DATA

DETERMINING WHETHER THE ENCODED DATA INCLUDES A DISABLE COMMAND

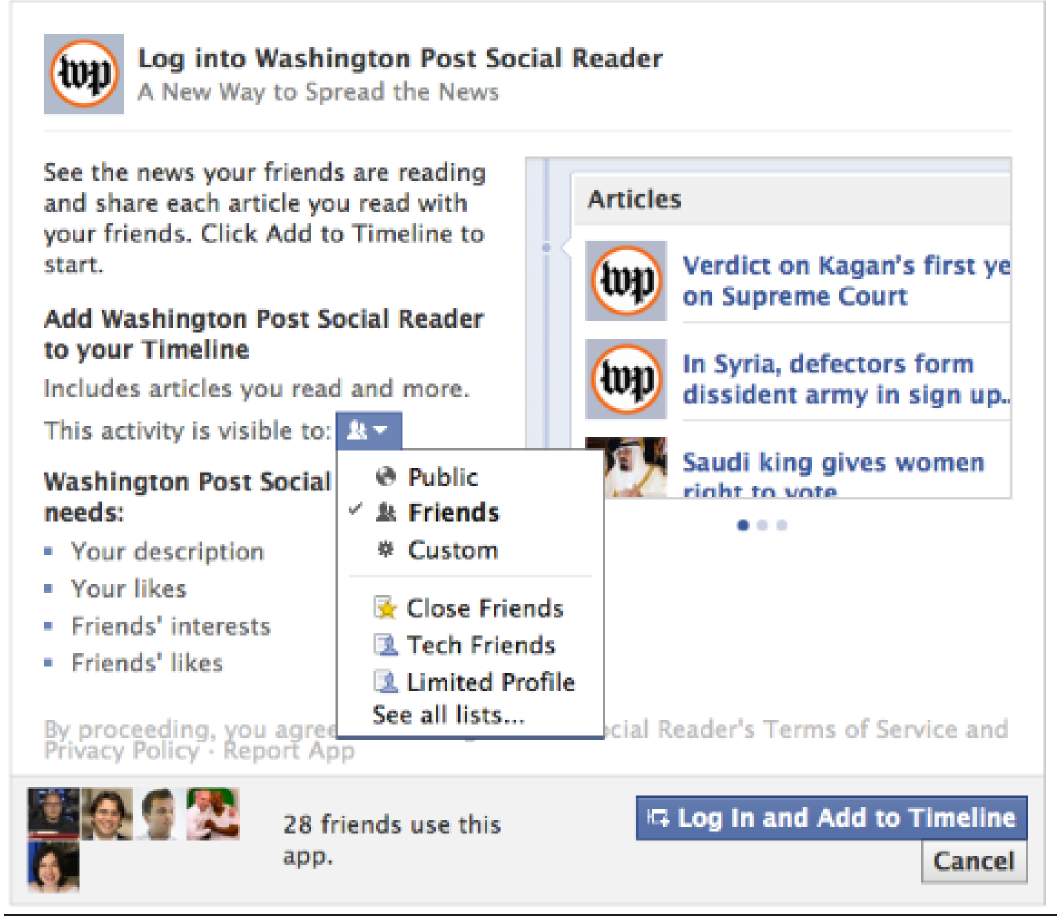
DISABLING A RECORD FUNCTION

Patently Apple

Apple's “Systems and Methods for Receiving Infrared Data with a Camera Design to Detect Images Based on Visible Light”

http://www.patentlyapple.com/patently-apple/2011/06
/apple-working-on-a-sophisticated-infrared-system-for-ios-cameras.html
http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2F
netahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220110128384%22.PGNR.&OS=DN/20110128384&RS=DN/20110128384

Take Control



Log into Washington Post Social Reader

A New Way to Spread the News

See the news your friends are reading and share each article you read with your friends. Click Add to Timeline to start.

Add Washington Post Social Reader to your Timeline

Includes articles you read and more.

This activity is visible to:

Washington Post Social needs:

- Your description
- Your likes
- Friends' interests
- Friends' likes

By proceeding, you agree cial Reader's Terms of Service and Privacy Policy · Report App

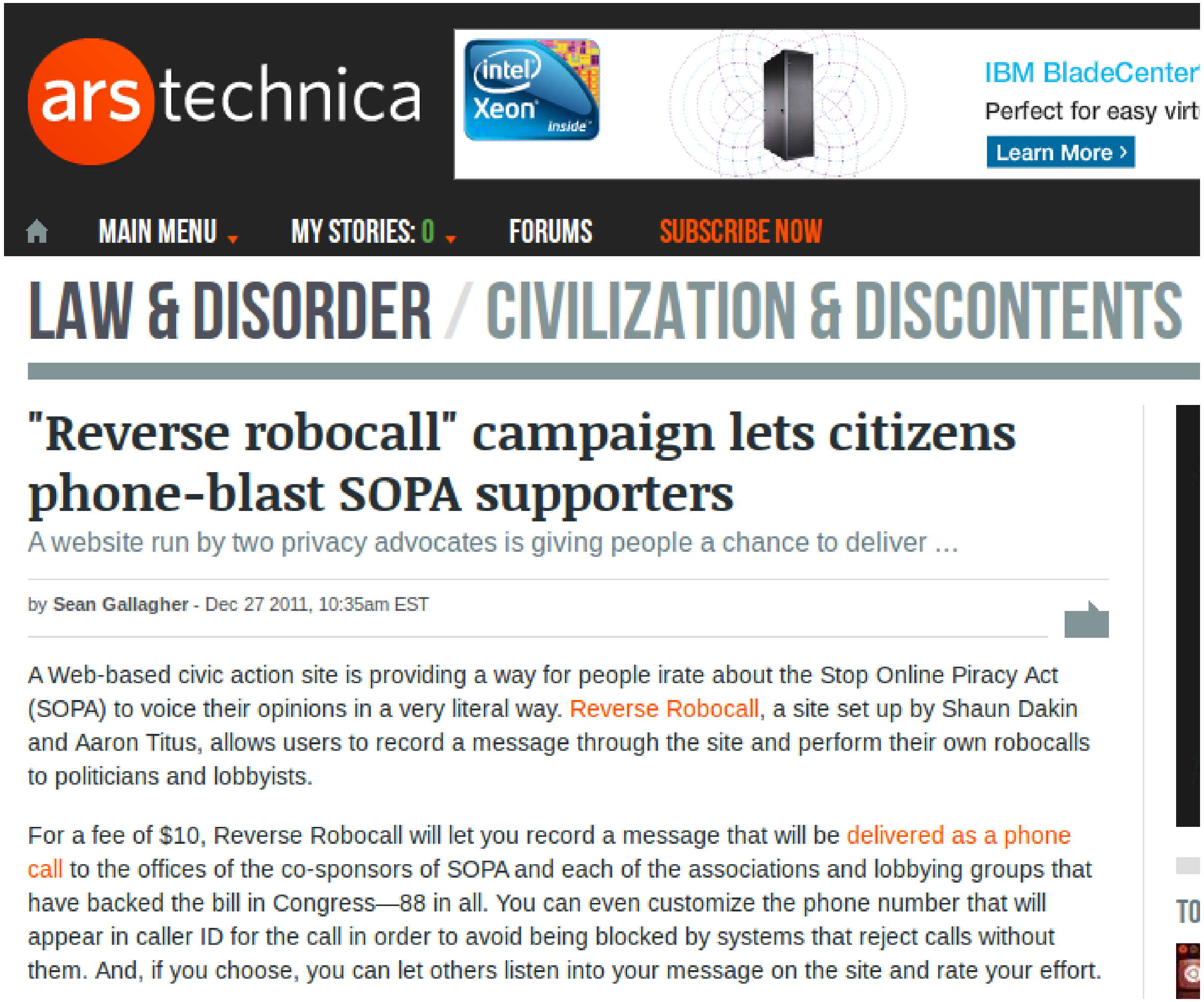
28 friends use this app.

Public
✓ Friends
Custom
Close Friends
Tech Friends
Limited Profile
See all lists...
Articles
Verdict on Kagan's first ye on Supreme Court
In Syria, defectors form dissident army in sign up..
Saudi king gives women right to vote
Log In and Add to Timeline
Cancel

But beware the illusion of control

http://mashable.com/2011/09/28/new-facebook/#27485Controlling-Who-Sees-Your-Activity

DOS
(The Human and the Communication Channel)



"Reverse robocall" campaign lets citizens phone-blast SOPA supporters

A website run by two privacy advocates is giving people a chance to deliver ...

by **Sean Gallagher** - Dec 27 2011, 10:35am EST

A Web-based civic action site is providing a way for people irate about the Stop Online Piracy Act (SOPA) to voice their opinions in a very literal way. Reverse Robocall, a site set up by Shaun Dakin and Aaron Titus, allows users to record a message through the site and perform their own robocalls to politicians and lobbyists.

For a fee of $10, Reverse Robocall will let you record a message that will be delivered as a phone call to the offices of the co-sponsors of SOPA and each of the associations and lobbying groups that have backed the bill in Congress—88 in all. You can even customize the phone number that will appear in caller ID for the call in order to avoid being blocked by systems that reject calls without them. And, if you choose, you can let others listen into your message on the site and rate your effort.

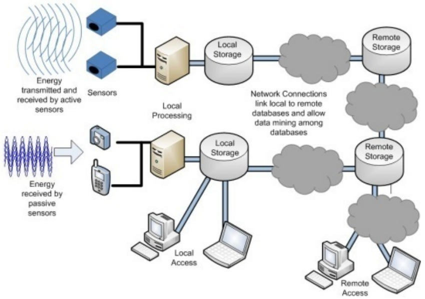
Reverse Robocall

http://arstechnica.com/tech-policy/2011/12/reverse-robocall-campaign-lets-citizens-phone-blast-sopa-supporters/

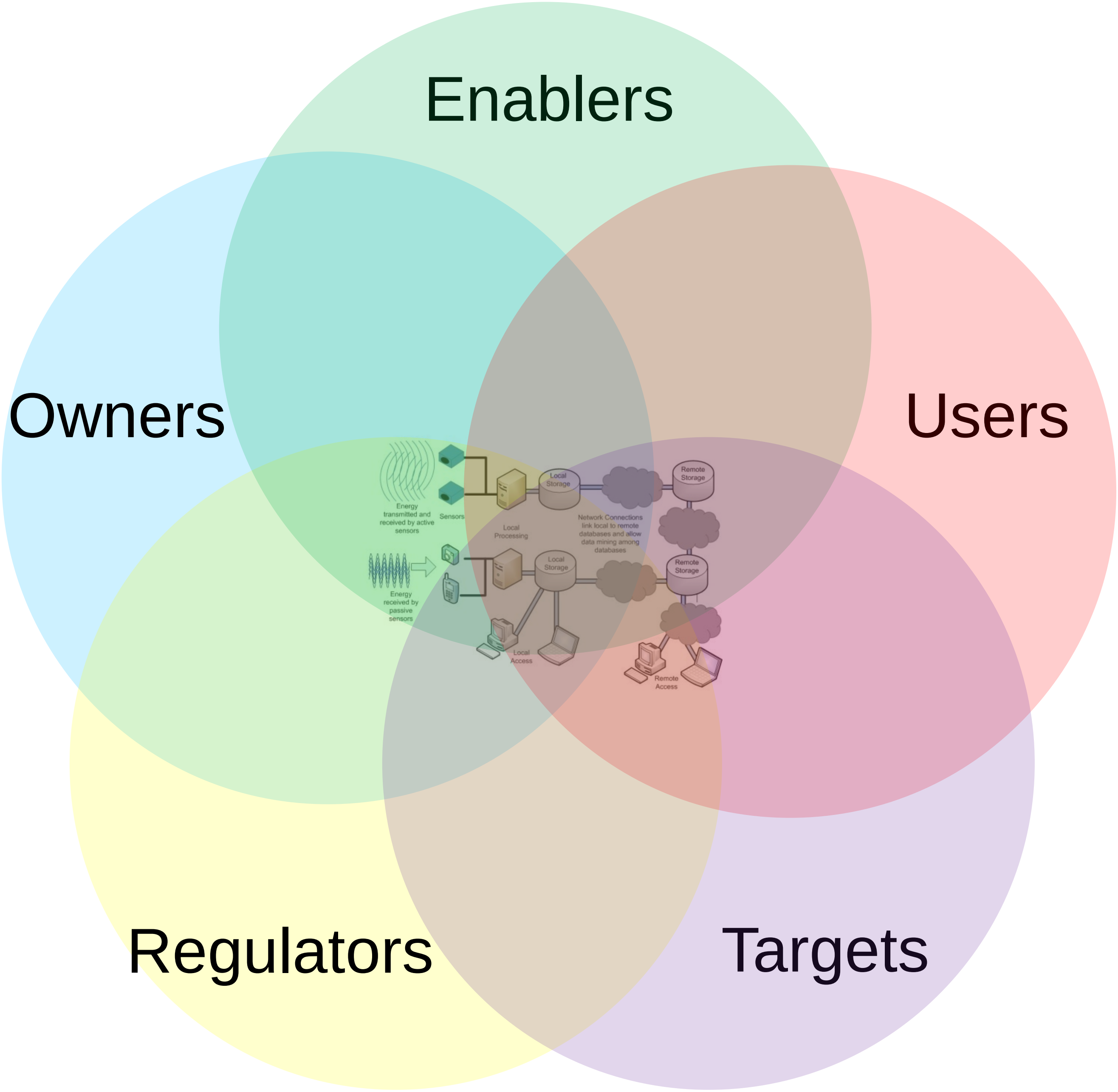
Understand the Actors

- Owners
- Enablers / Purveyors
- Information Consumers
- Regulators
- Targets (the Surveilled)

Model in Context


Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access

Model in Context



Enablers

Owners

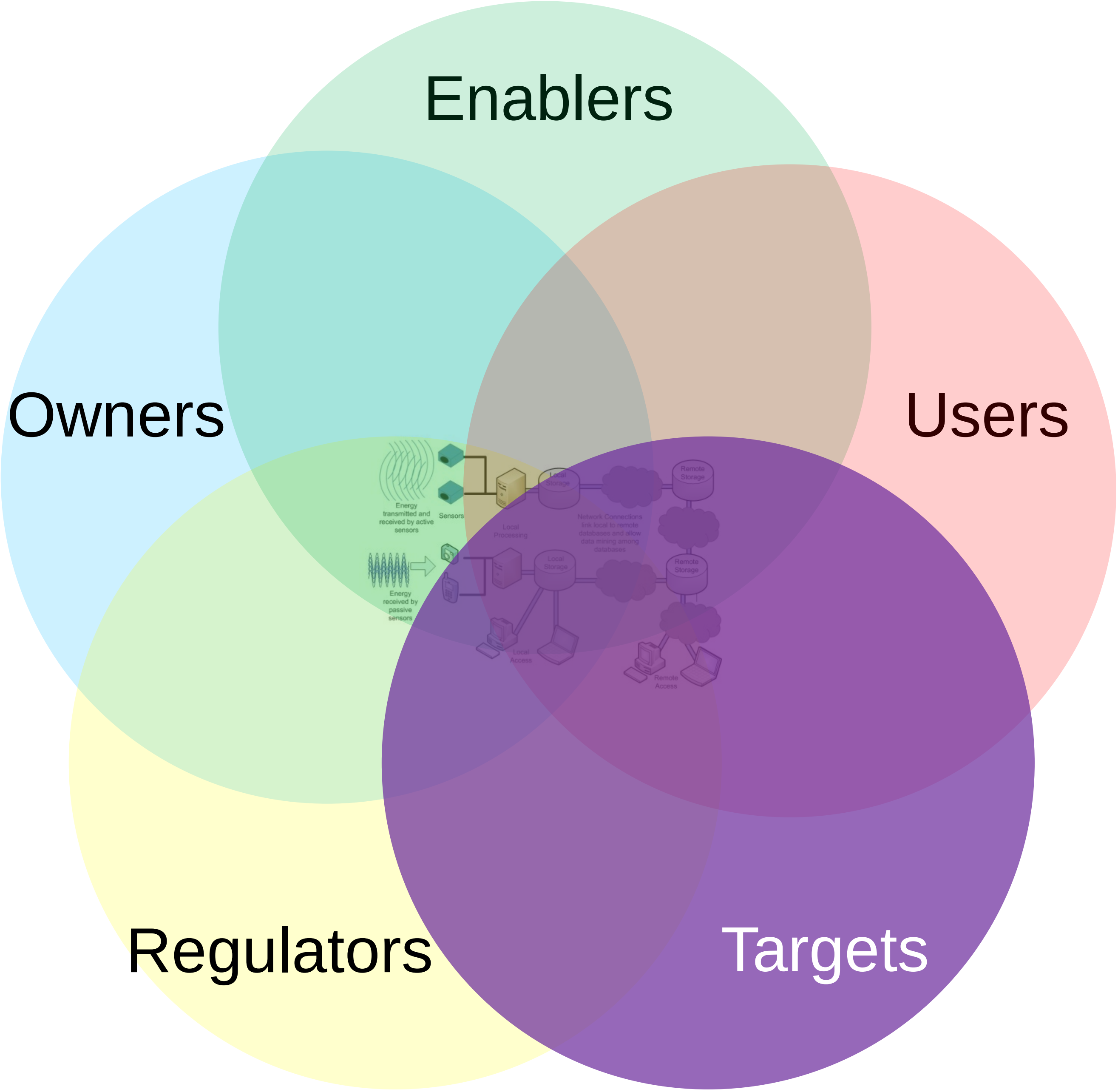
Users

Regulators

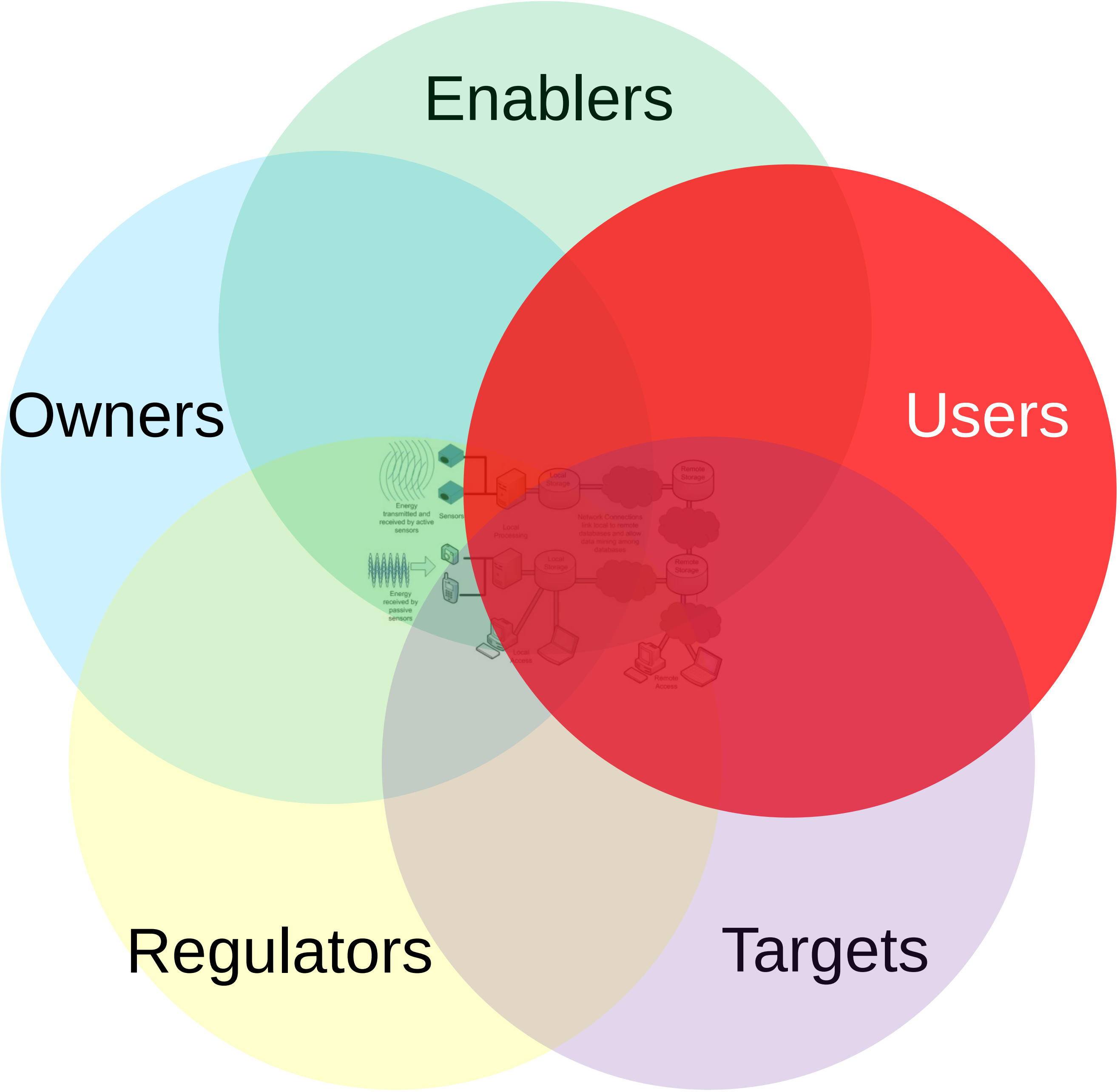
Targets

Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Network Connections link local to remote databases and allow data mining among databases
Remote Storage
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access

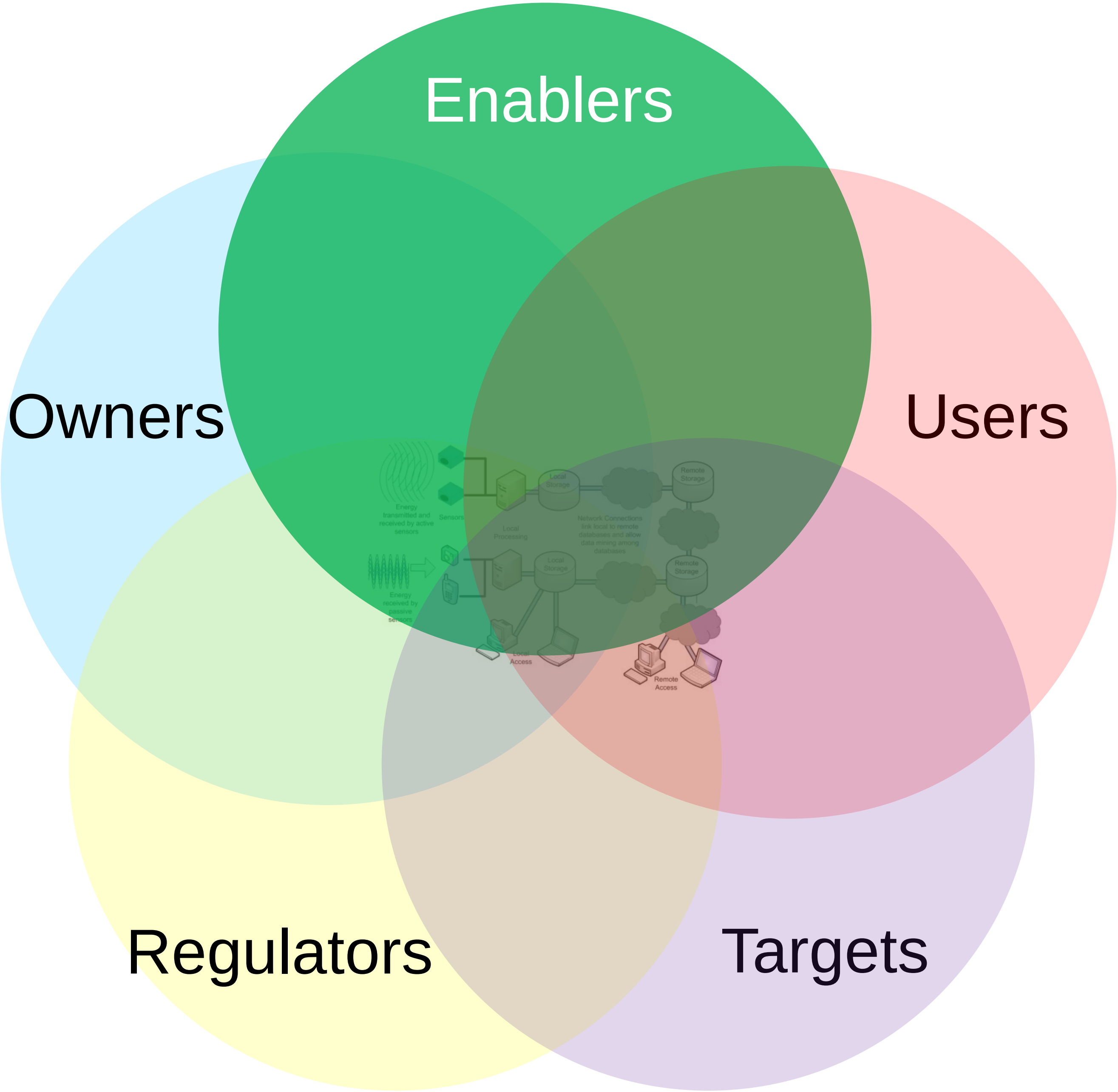
Model in Context


Enablers
Owners
Users
Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access
Regulators
Targets

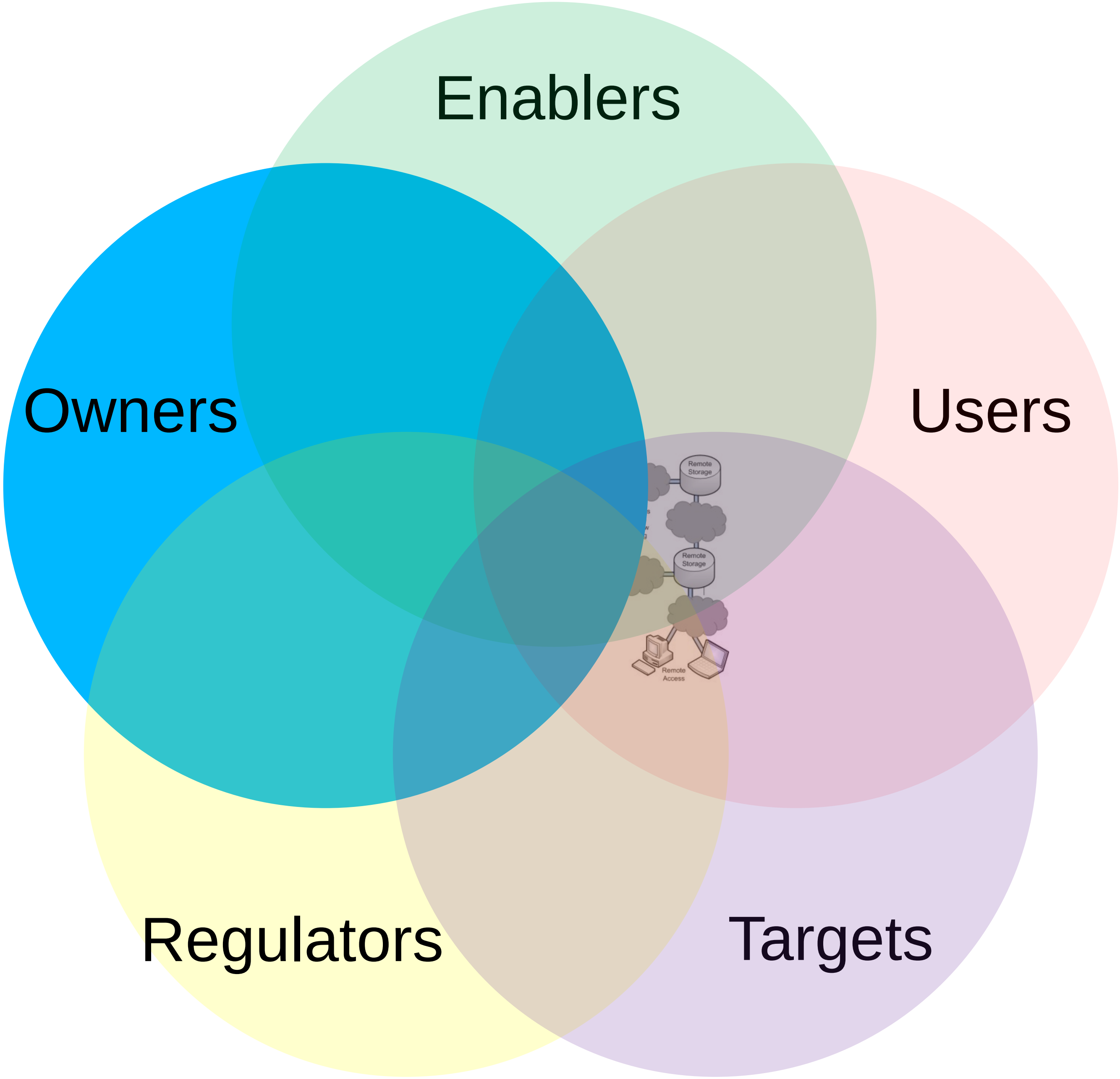
Model in Context


Enablers
Owners
Users
Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Local Storage
Remote Storage
Energy received by passive sensors
Local Access
Remote Access
Regulators
Targets

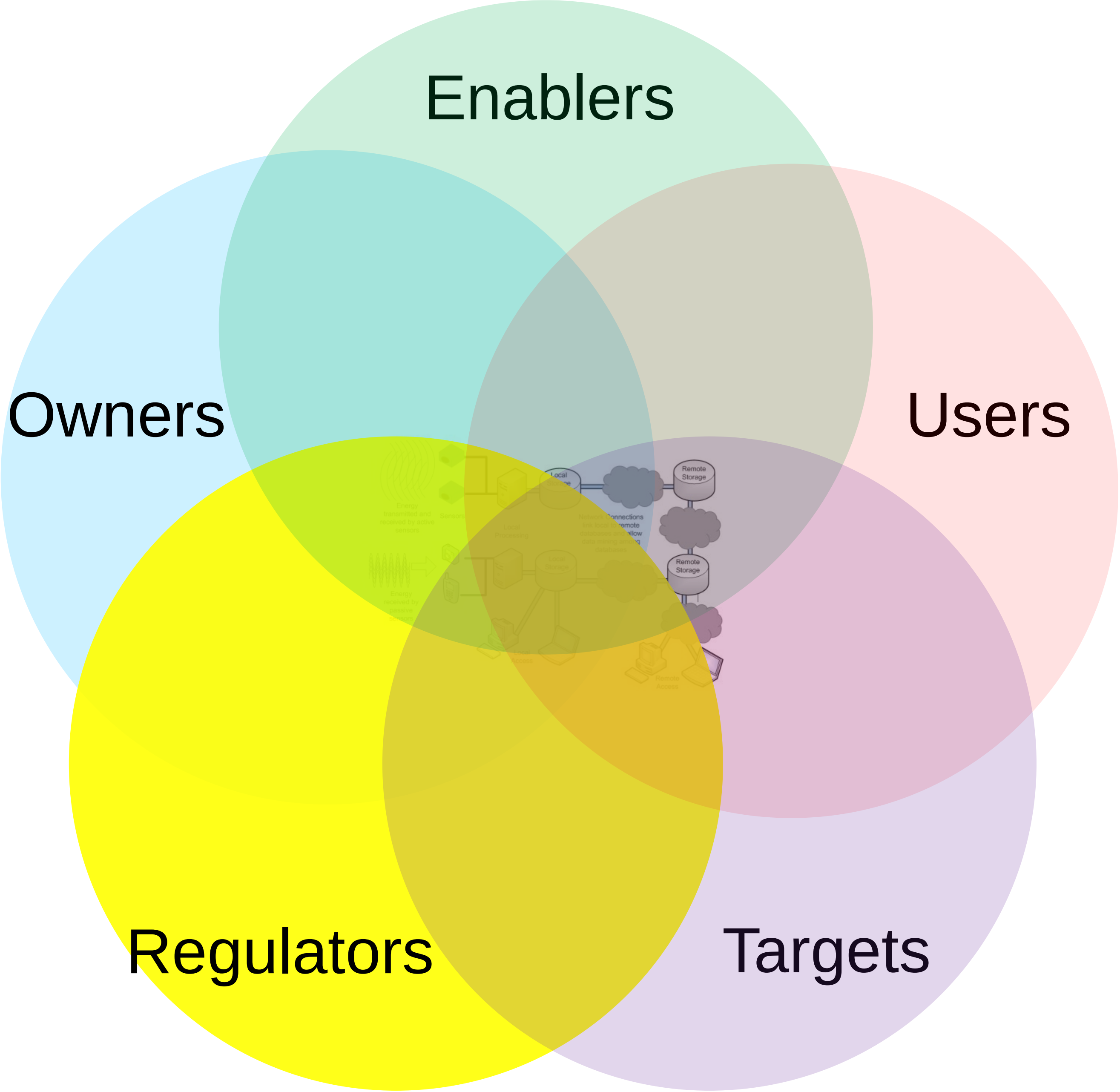
Model in Context


Enablers
Owners
Users
Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Network Connections link local to remote databases and allow data mining among databases
Remote Storage
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access
Regulators
Targets

Model in Context



Model in Context

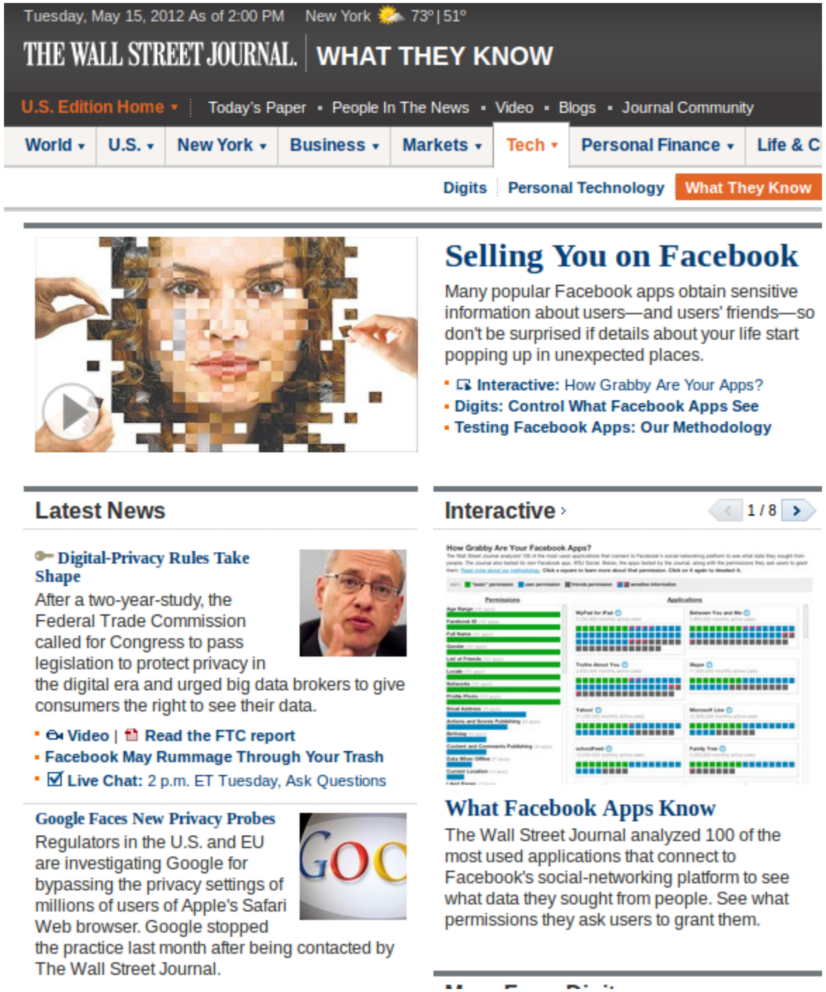

Enablers
Owners
Users
Regulators
Targets
Energy transmitted and received by active sensors
Sensors
Local Processing
Local Storage
Remote Storage
Network Connections link local to remote databases and allow data mining among databases
Energy received by passive sensors
Local Storage
Remote Storage
Local Access
Remote Access

Influence Policy and Policy Makers

Vote

http://en.wikipedia.org/wiki/File:Election_MG_3455.JPG

Educate



Tuesday, May 15, 2012 As of 2:00 PM New York 73° | 51°

THE WALL STREET JOURNAL. | WHAT THEY KNOW

U.S. Edition Home ▾ | Today's Paper • People In The News • Video • Blogs • Journal Community

World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life & C

Digits | Personal Technology | What They Know

Selling You on Facebook

Many popular Facebook apps obtain sensitive information about users—and users' friends—so don't be surprised if details about your life start popping up in unexpected places.

- Interactive: How Grabby Are Your Apps?
- Digits: Control What Facebook Apps See
- Testing Facebook Apps: Our Methodology

Latest News

Digital-Privacy Rules Take Shape

After a two-year-study, the Federal Trade Commission called for Congress to pass legislation to protect privacy in the digital era and urged big data brokers to give consumers the right to see their data.

- Video | Read the FTC report
- Facebook May Rummage Through Your Trash
- Live Chat: 2 p.m. ET Tuesday, Ask Questions

Google Faces New Privacy Probes

Regulators in the U.S. and EU are investigating Google for bypassing the privacy settings of millions of users of Apple's Safari Web browser. Google stopped the practice last month after being contacted by The Wall Street Journal.

Interactive ›

1 / 8

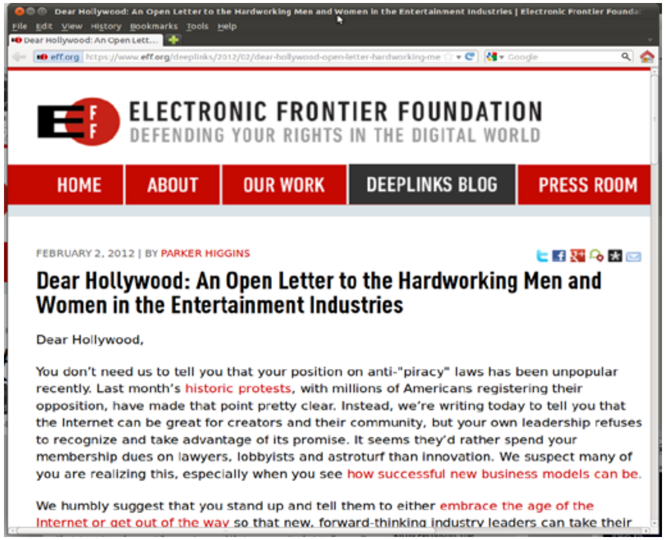
How Grabby Are Your Facebook Apps?

What Facebook Apps Know

The Wall Street Journal analyzed 100 of the most used applications that connect to Facebook's social-networking platform to see what data they sought from people. See what permissions they ask users to grant them.

Media

See Stephen Cass' excellent "How to Talk to the Mainstream Media" from The Last HOPE



Dear Hollywood: An Open Letter to the Hardworking Men and Women in the Entertainment Industries | Electronic Frontier Founda

File Edit View History Bookmarks Tools Help

https://www.eff.org/deeplinks/2012/02/dear-hollywood-open-letter-hardworking-me

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM

FEBRUARY 2, 2012 | BY PARKER HIGGINS

Dear Hollywood: An Open Letter to the Hardworking Men and Women in the Entertainment Industries

Dear Hollywood,

You don't need us to tell you that your position on anti-"piracy" laws has been unpopular recently. Last month's historic protests, with millions of Americans registering their opposition, have made that point pretty clear. Instead, we're writing today to tell you that the Internet can be great for creators and their community, but your own leadership refuses to recognize and take advantage of its promise. It seems they'd rather spend your membership dues on lawyers, lobbyists and astroturf than innovation. We suspect many of you are realizing this, especially when you see how successful new business models can be.

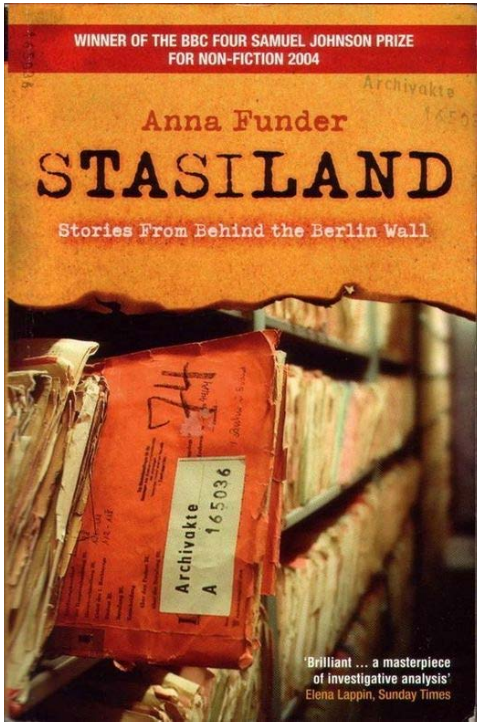
We humbly suggest that you stand up and tell them to either embrace the age of the Internet or get out of the way so that new, forward-thinking industry leaders can take their

Communities

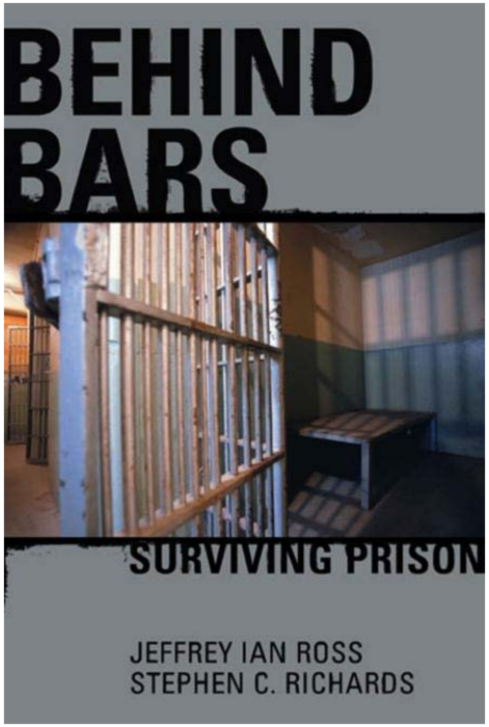
Decision Makers

http://www.senaterepublicans.wa.gov/news/2011/fain/031511TH.htm

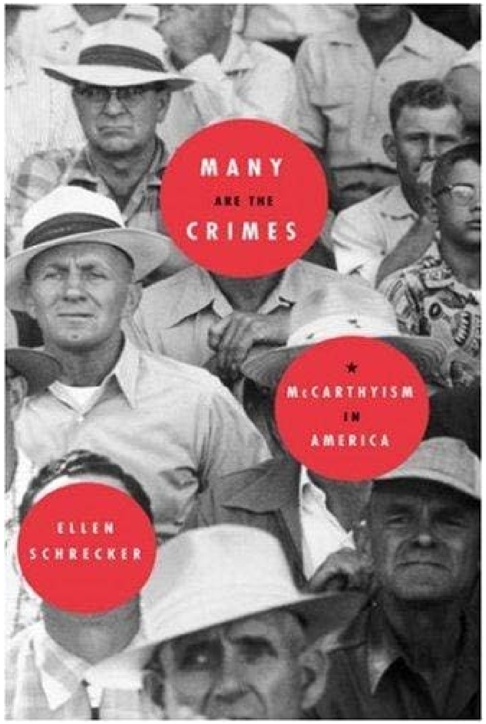
Look to History and Surveillance Cultures


WINNER OF THE BBC FOUR SAMUEL JOHNSON PRIZE FOR NON-FICTION 2004
Anna Funder
STASILAND
Stories From Behind the Berlin Wall
Archivakte A 165036
'Brilliant ... a masterpiece of investigative analysis'
Elena Lappin, Sunday Times

East Germany

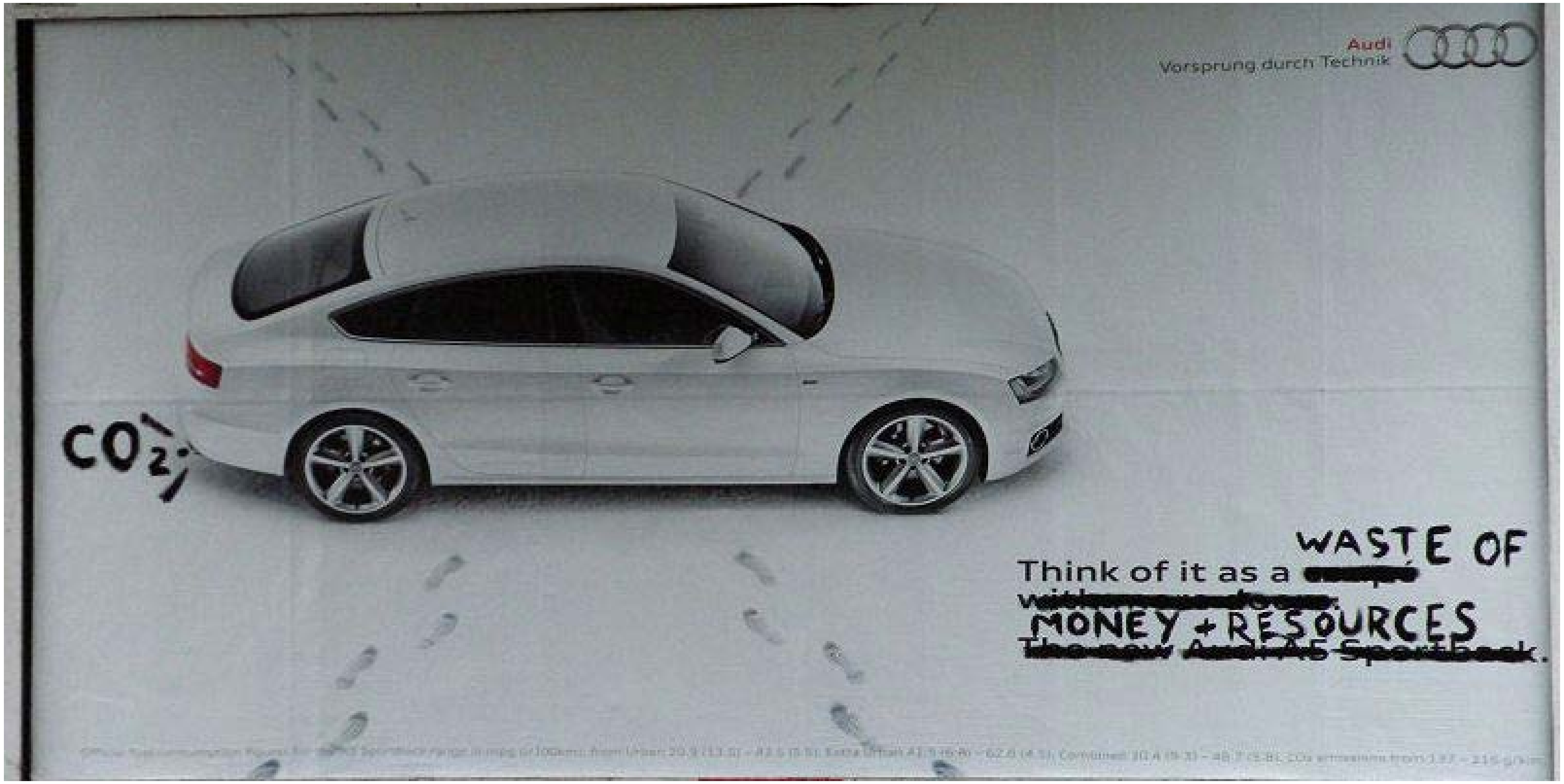


Prison



McCarthy-era

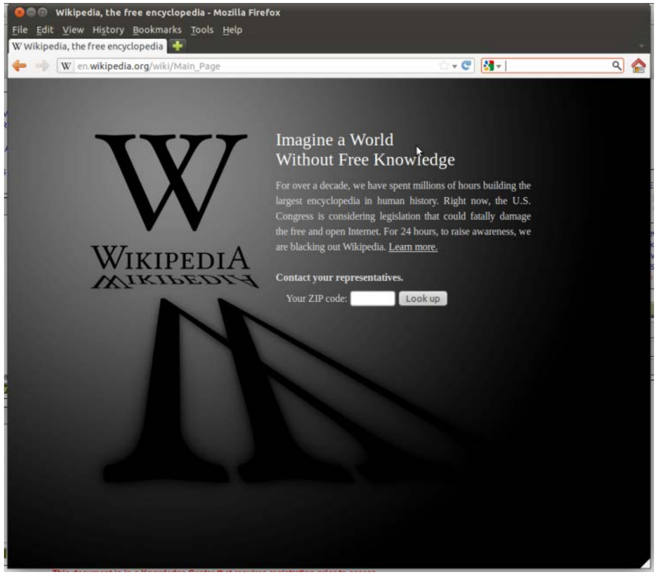
Culture Jamming


Audi
Vorsprung durch Technik
CO2
Think of it as a [redacted] WASTE OF
[redacted]
MONEY + RESOURCES
~~The new Audi A5 Sportback~~.

Graffiti on Billboard in Cambridge, UK

http://en.wikipedia.org/wiki/File:Vorsprung_durch_Graffit_-_geograph.org.uk_-_1670605.jpg

Rally Support

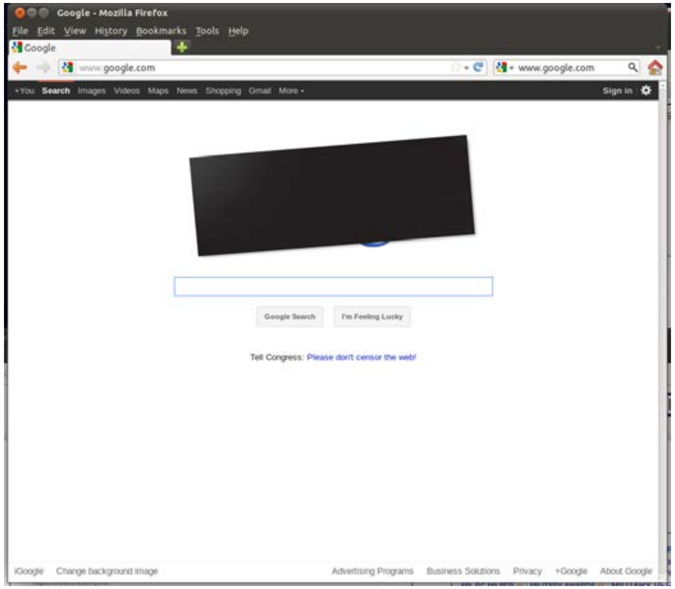

Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Main_Page
Wikipedia

Imagine a World
Without Free Knowledge

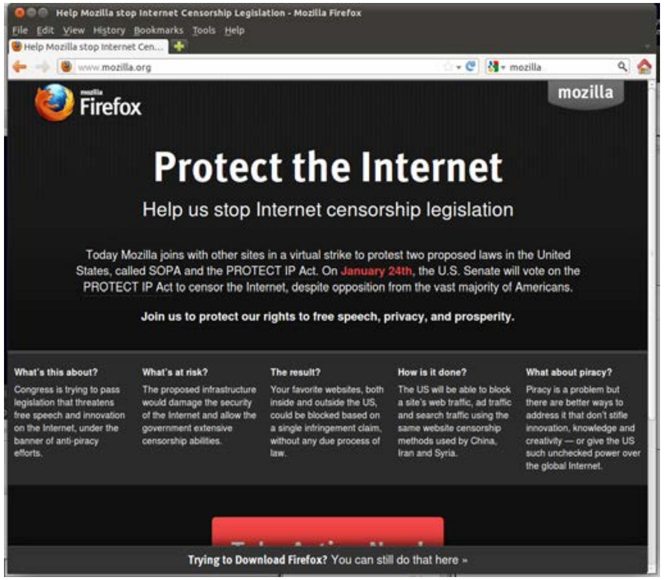
For over a decade, we have spent millions of hours building the largest encyclopedia in human history. Right now, the U.S. Congress is considering legislation that could fatally damage the free and open Internet. For 24 hours, to raise awareness, we are blacking out Wikipedia. Learn more.

Contact your representatives.

Your ZIP code: Look up


Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
www.google.com
www.google.com
+You Search Images Videos Maps News Shopping Gmail More
Sign in
Google Search
I'm Feeling Lucky
iGoogle Change background image
Advertising Programs Business Solutions Privacy +Google About Google

Tell Congress: Please don't censor the web!


Help Mozilla stop Internet Censorship Legislation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Help Mozilla stop Internet Cen...
www.mozilla.org
mozilla
mozilla Firefox
mozilla

Protect the Internet

Help us stop Internet censorship legislation

Today Mozilla joins with other sites in a virtual strike to protest two proposed laws in the United States, called SOPA and the PROTECT IP Act. On January 24th, the U.S. Senate will vote on the PROTECT IP Act to censor the Internet, despite opposition from the vast majority of Americans.

Join us to protect our rights to free speech, privacy, and prosperity.

What's this about?
Congress is trying to pass legislation that threatens free speech and innovation on the Internet, under the banner of anti-piracy efforts.

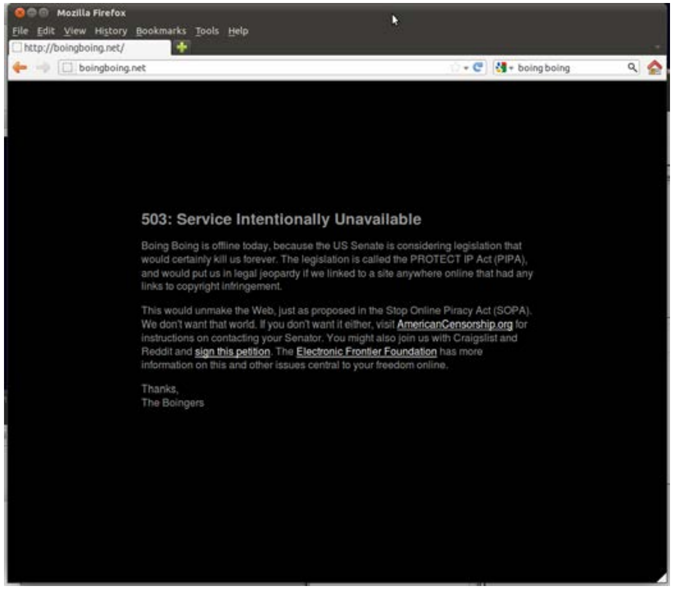
What's at risk?
The proposed infrastructure would damage the security of the Internet and allow the government extensive censorship abilities.

The result?
Your favorite websites, both inside and outside the US, could be blocked based on a single infringement claim, without any due process of law.

How is it done?
The US will be able to block a site's web traffic, ad traffic and search traffic using the same website censorship methods used by China, Iran and Syria.

What about piracy?
Piracy is a problem but there are better ways to address it that don't stifle innovation, knowledge and creativity — or give the US such unchecked power over the global Internet.

Trying to Download Firefox? You can still do that here »



503: Service Intentionally Unavailable

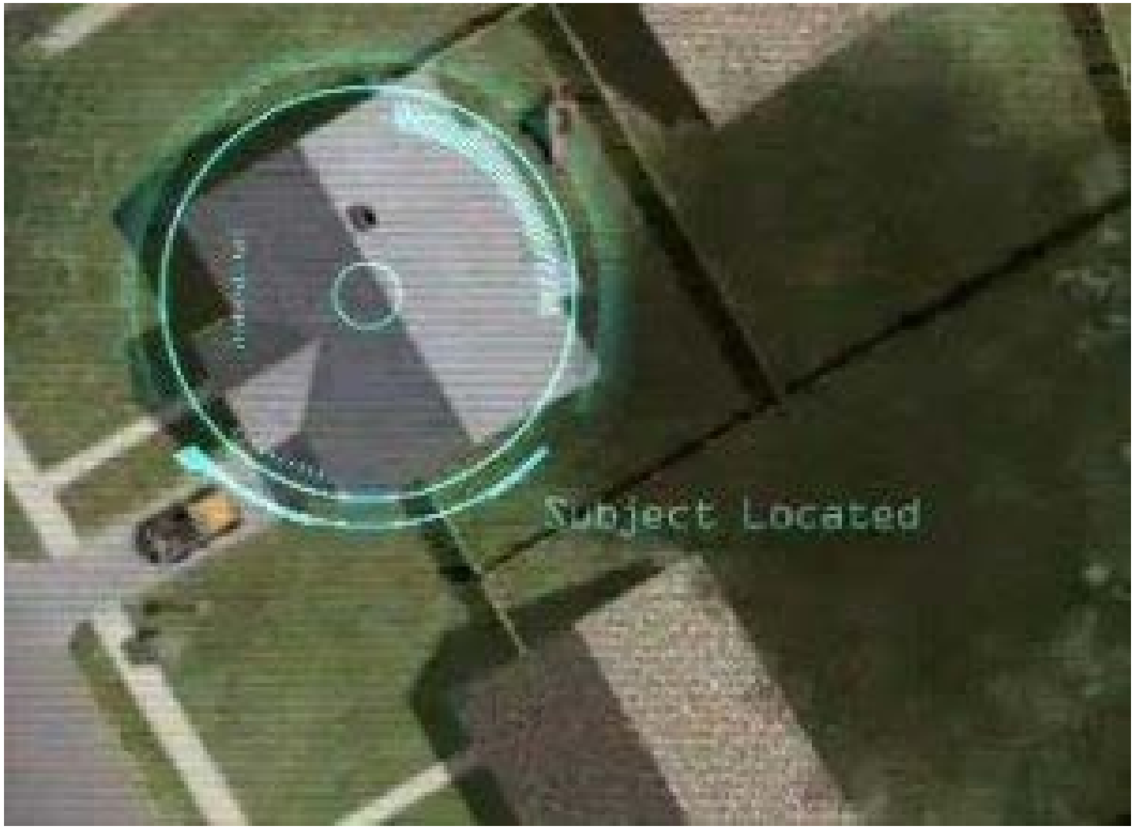
Boing Boing is offline today, because the US Senate is considering legislation that would certainly kill us forever. The legislation is called the PROTECT IP Act (PIPA), and would put us in legal jeopardy if we linked to a site anywhere online that had any links to copyright infringement.

This would unmake the Web, just as proposed in the Stop Online Piracy Act (SOPA). We don't want that world. If you don't want it either, visit AmericanCensorship.org for instructions on contacting your Senator. You might also join us with Craigslist and Reddit and sign this petition. The Electronic Frontier Foundation has more information on this and other issues central to your freedom online.

Thanks,
The Boingers

Stop Online Piracy Act (SOPA) Blackout Day – 18 January 2012

Cry Foul...



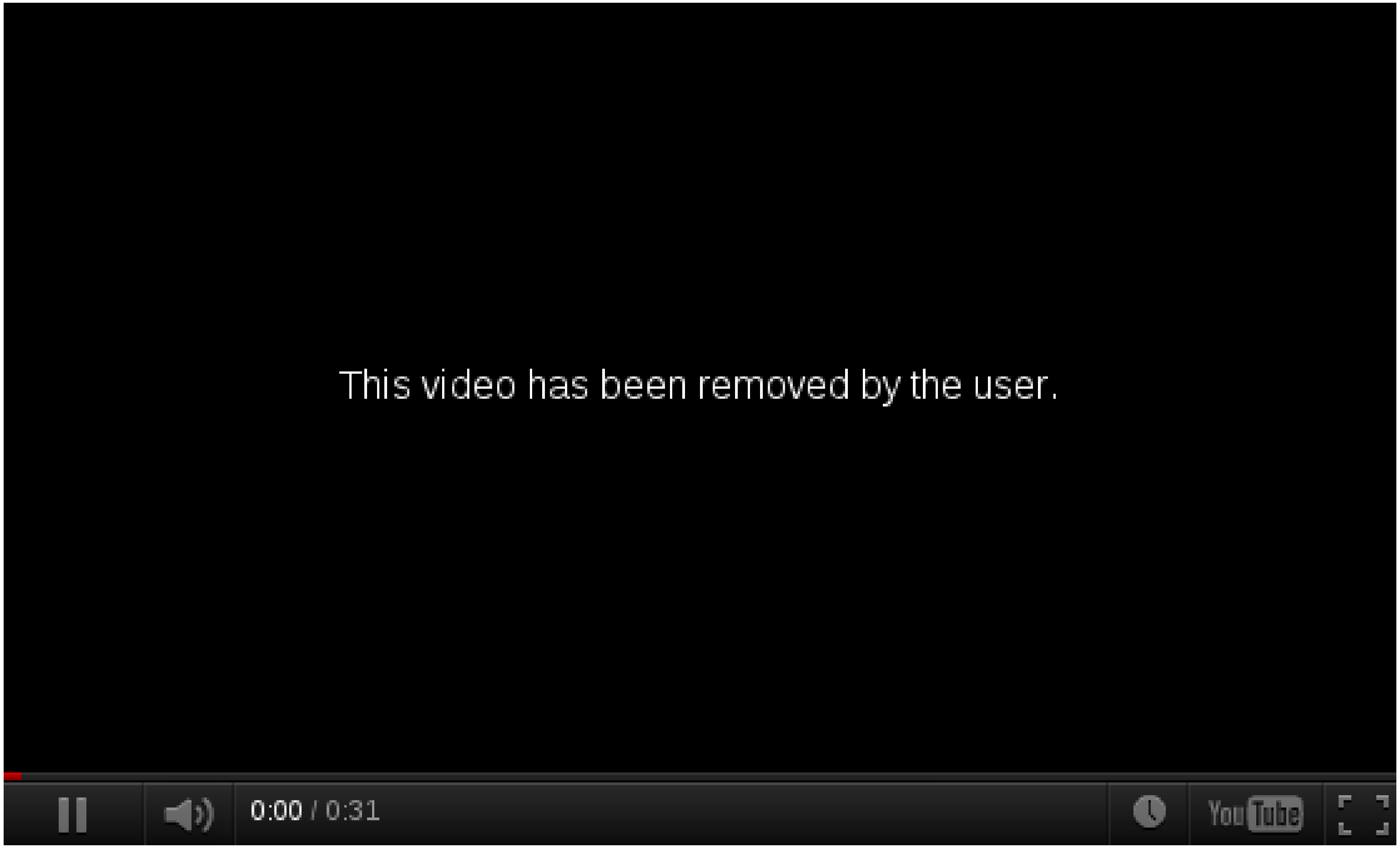
"Listen, Tom, we can make this easy," the voice says as a satellite image zooms in from space onto Tom's house.

"Tom, we do know who you are," the narrator continues before a caption appears on the screen, "Find us before we find you."

PA Tax Amnesty TV ad “We Know Who You Are”

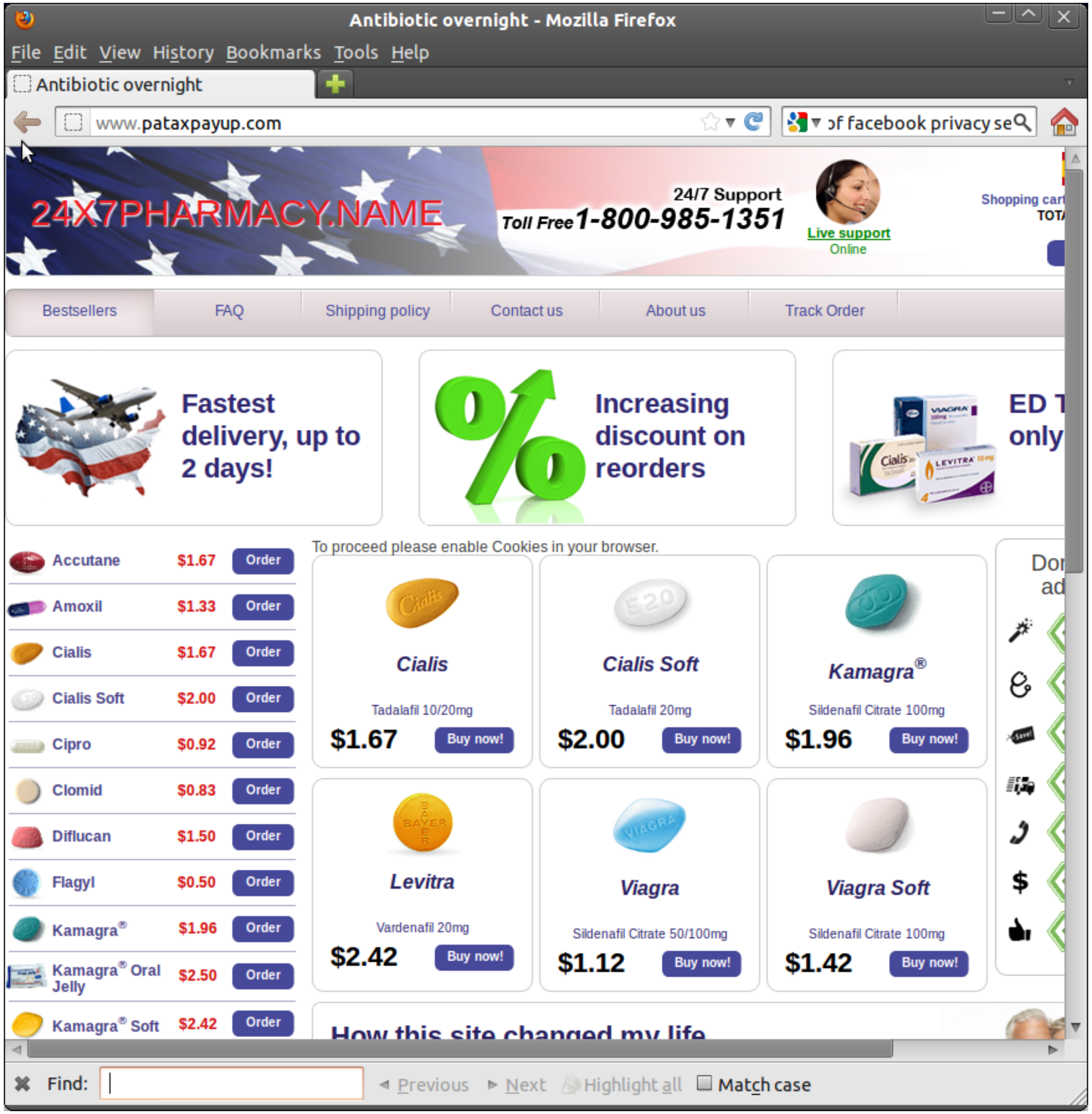
http://www.huffingtonpost.com/2010/05/02/pennsylvania-tax-ad-has-o_n_560178.html

And Sometimes it Will Have the Desired Effect...



This video has been removed by the user.

And Sometimes it Will Have the Desired Effect...



Accutane	$1.67	Order
Amoxil	$1.33	Order
Cialis	$1.67	Order
Cialis Soft	$2.00	Order
Cipro	$0.92	Order
Clomid	$0.83	Order
Diflucan	$1.50	Order
Flagyl	$0.50	Order
Kamagra®	$1.96	Order
Kamagra® Oral Jelly	$2.50	Order
Kamagra® Soft	$2.42	Order

To proceed please enable Cookies in your browser.

Cialis Tadalafil 10/20mg $1.67 Buy now!	Cialis Soft Tadalafil 20mg $2.00 Buy now!	Kamagra® Sildenafil Citrate 100mg $1.96 Buy now!
Levitra Vardenafil 20mg $2.42 Buy now!	Viagra Sildenafil Citrate 50/100mg $1.12 Buy now!	Viagra Soft Sildenafil Citrate 100mg $1.42 Buy now!

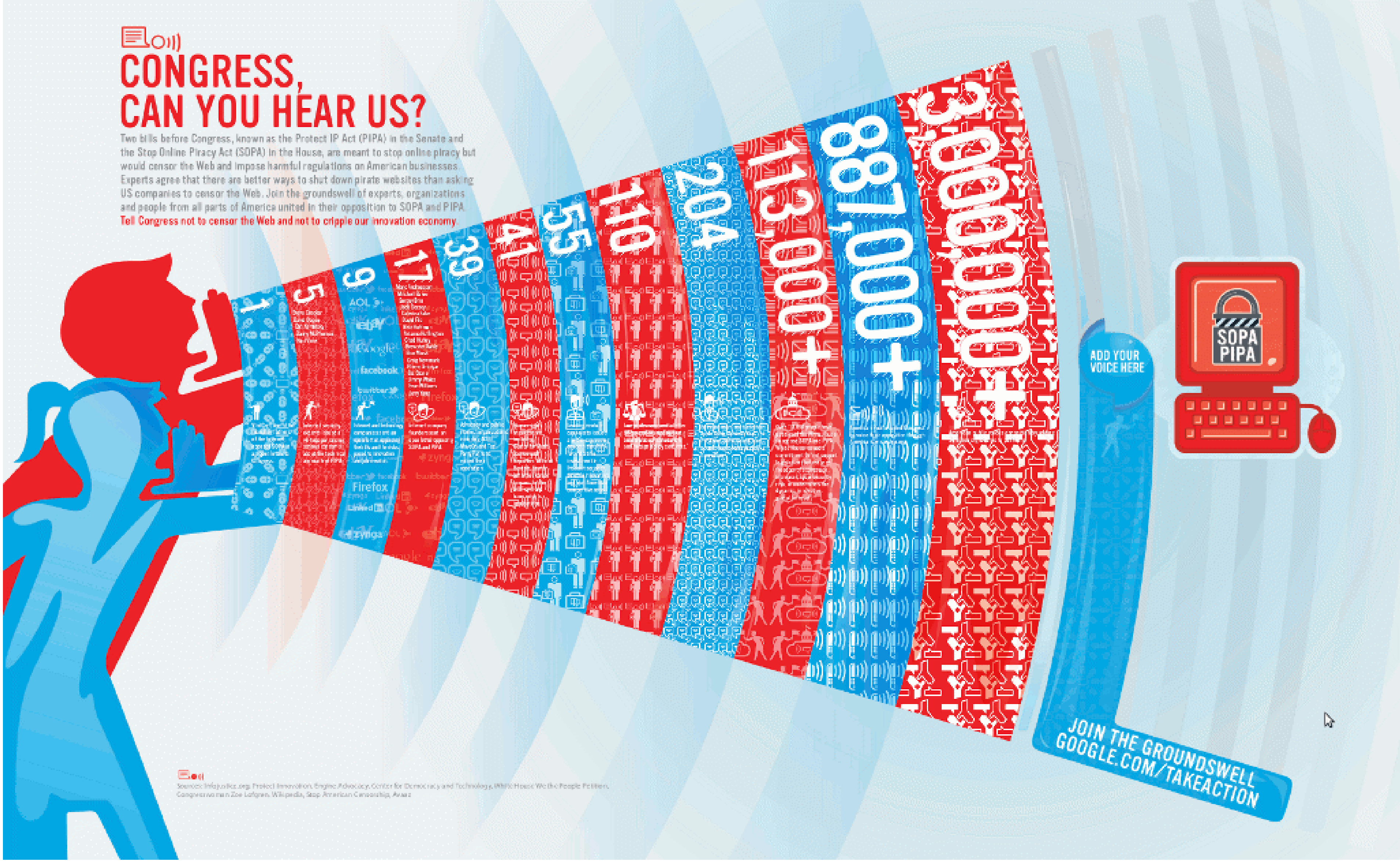
How this site changed my life

http://www.pataxpayup.com/

But Communicate Issues Effectively

See "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy"
by Daniel Solove for one powerful example.

Art is Powerful



CONGRESS,
CAN YOU HEAR US?

Two bills before Congress, known as the Protect IP Act (PIPA) in the Senate and the Stop Online Piracy Act (SOPA) in the House, are meant to stop online piracy but would censor the Web and impose harmful regulations on American businesses. Experts agree that there are better ways to shut down pirate websites than asking US companies to censor the Web. Join the groundswell of experts, organizations and people from all parts of America united in their opposition to SOPA and PIPA. Tell Congress not to censor the Web and not to cripple our innovation economy.

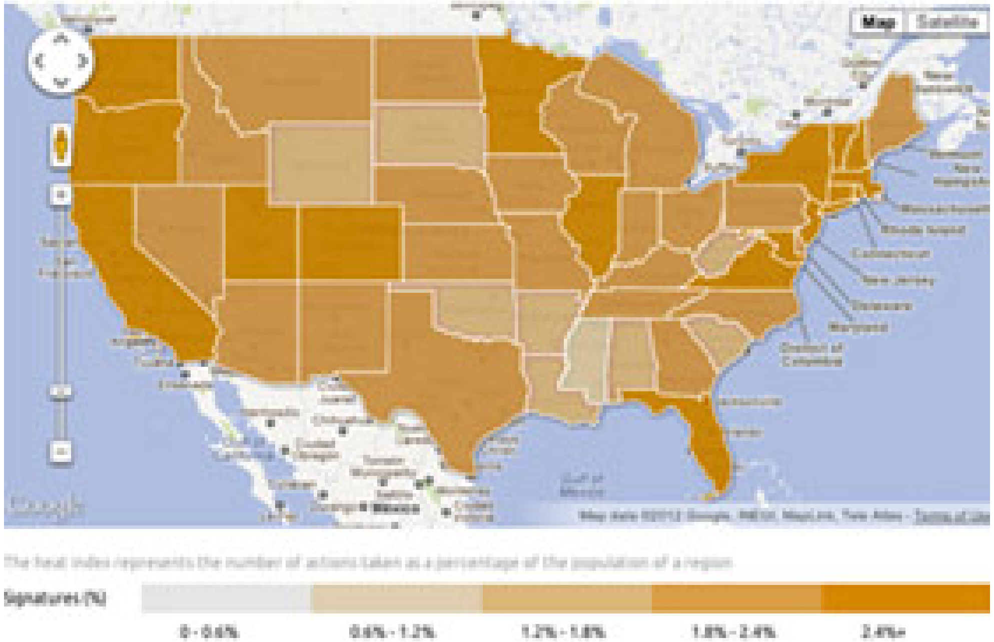
Sources: Infojustice.org, Protect Innovation, Engine Advocacy, Center for Democracy and Technology, White House We the People Petition, Congresswoman Zoe Lofgren, Wikipedia, Stop American Censorship, Avaaz

https://www.google.com/takeaction/

Sometimes it Works

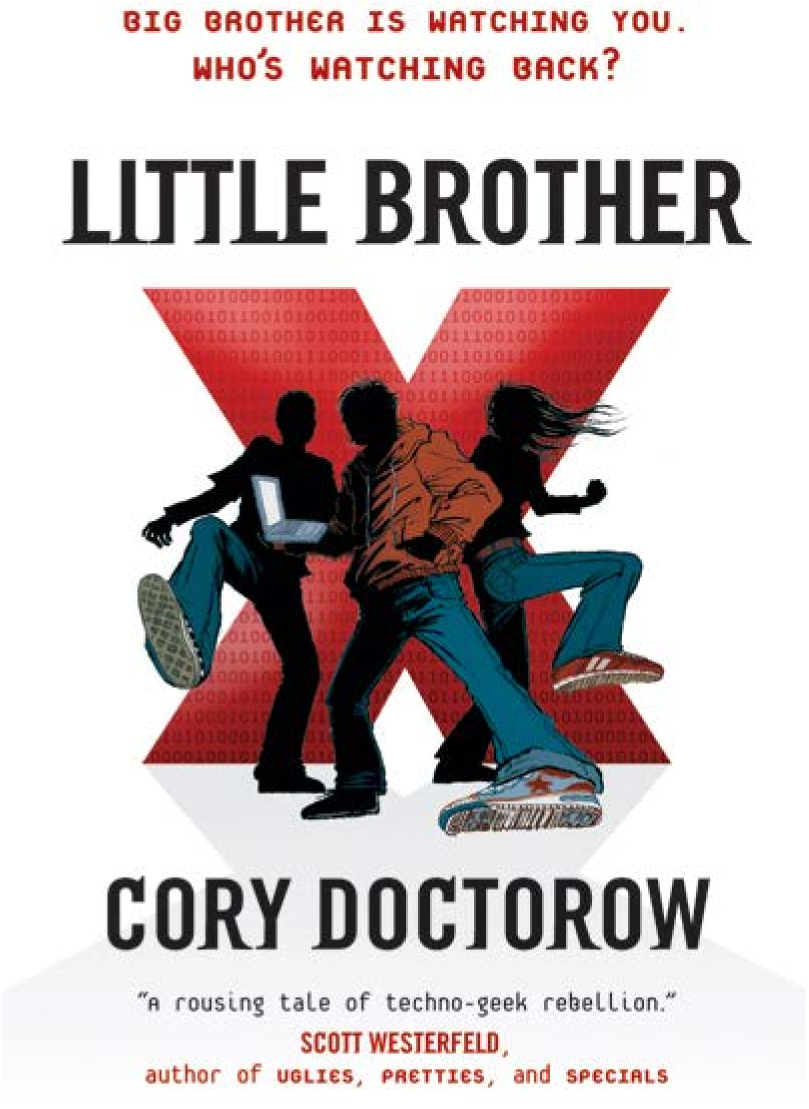
Thank you Congress

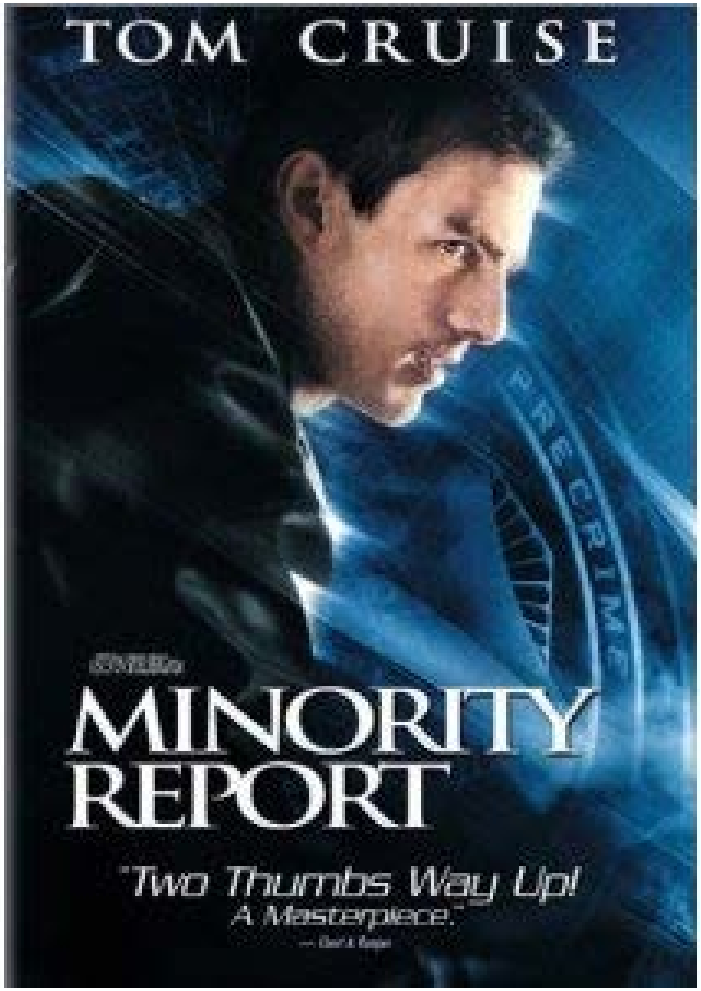
A groundswell of opposition against PIPA and SOPA.
Thank you – and the more than 7 million other Americans – who stood up for the Web.


Map
Satellite
Google
Gulf of Mexico
Map data ©2012 Google, INEGI, MapLink, Tele Atlas - Terms of Use
The heat index represents the number of actions taken as a percentage of the population of a region.
Signatures (%)
0 - 0.6%
0.6% - 1.2%
1.2% - 1.8%
1.8% - 2.4%
2.4%+

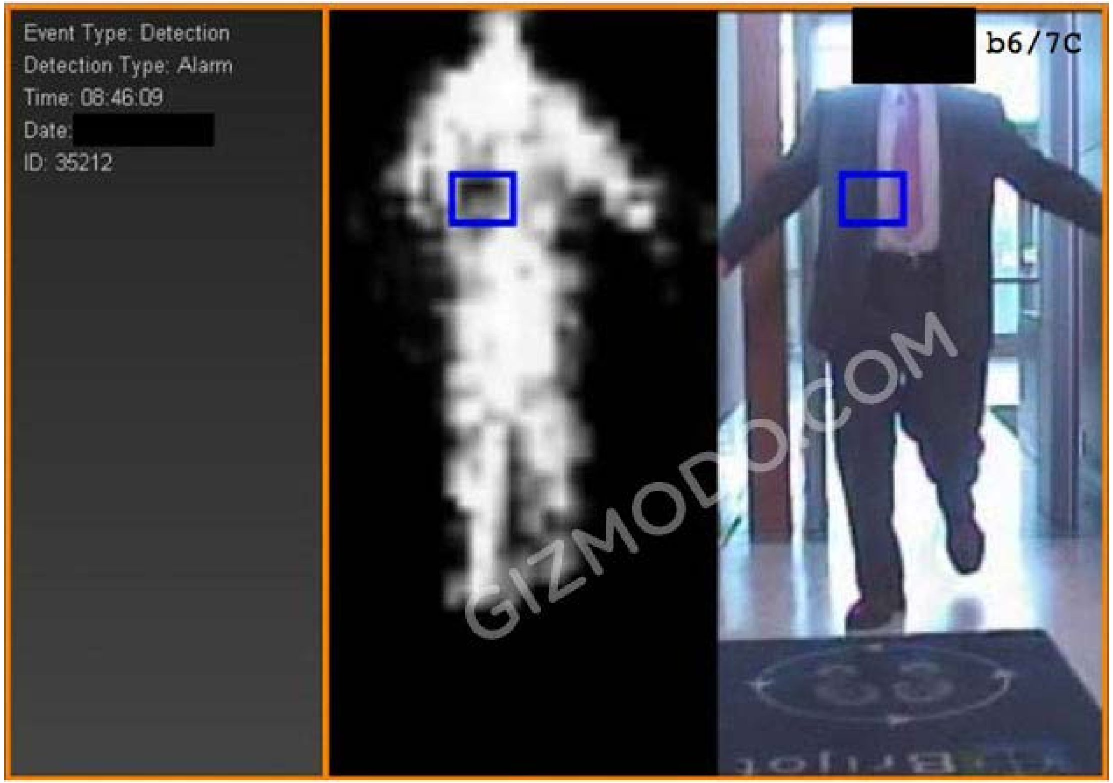
https://www.google.com/takeaction/

As is Science Fiction


BIG BROTHER IS WATCHING YOU.
WHO'S WATCHING BACK?
LITTLE BROTHER
CORY DOCTOROW
"A rousing tale of techno-geek rebellion."
SCOTT WESTERFELD,
author of UGLIES, PRETTIES, and SPECIALS



Highlight Costs, Effectiveness, Security and Health Risks



“100 Naked Citizens: 100 Leaked Body Scans”

“A Colorado teen is upset with screeners at Salt Lake City International Airport. The type one diabetic says TSA agents were abrupt, rude and were responsible for breaking her $10,000 insulin pump. A pump she has to have to survive. ”

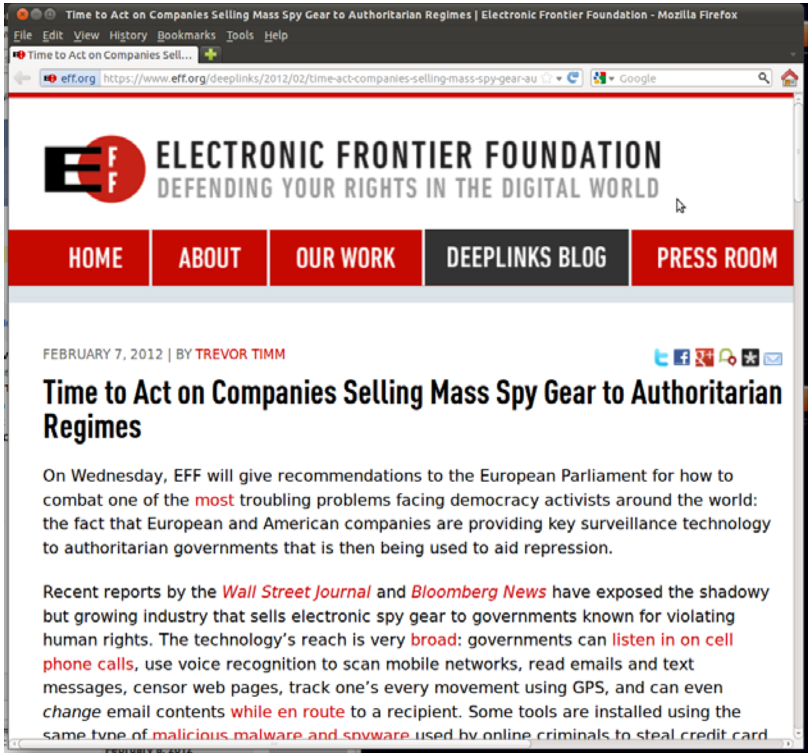
“... has spent nearly $90 million replacing traditional magnetometers with controversial X-ray body scanning machines...”

“FDA Leans on Device Makers To Cut X-Ray Doses For Kids”

“$1B of TSA Nude Body Scanners Made Worthless By Blog — How Anyone Can Get Anything Past The Scanners”

http://www.wired.com/threatlevel/2010/11/giz-scans/
http://www.wired.com/threatlevel/2012/05/body-scanner-vulnerabilities
http://www.abc4.com/content/news/state/story/TSA-diabetes-salt-lake-insulin-savannah/Az-QjubuEUeXMX7LAbC1Xw.cspx
http://www.npr.org/blogs/health/2012/05/09/152337190/fda-leans-on-device-makers-to-cut-x-ray-doses-for-kids?ft=1&f=152337190
http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners/

Transparency and Disclosure



Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes | Electronic Frontier Foundation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Time to Act on Companies Sell...
eff.org https://www.eff.org/deeplinks/2012/02/time-act-companies-selling-mass-spy-gear-au
Google
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM

FEBRUARY 7, 2012 | BY TREVOR TIMM

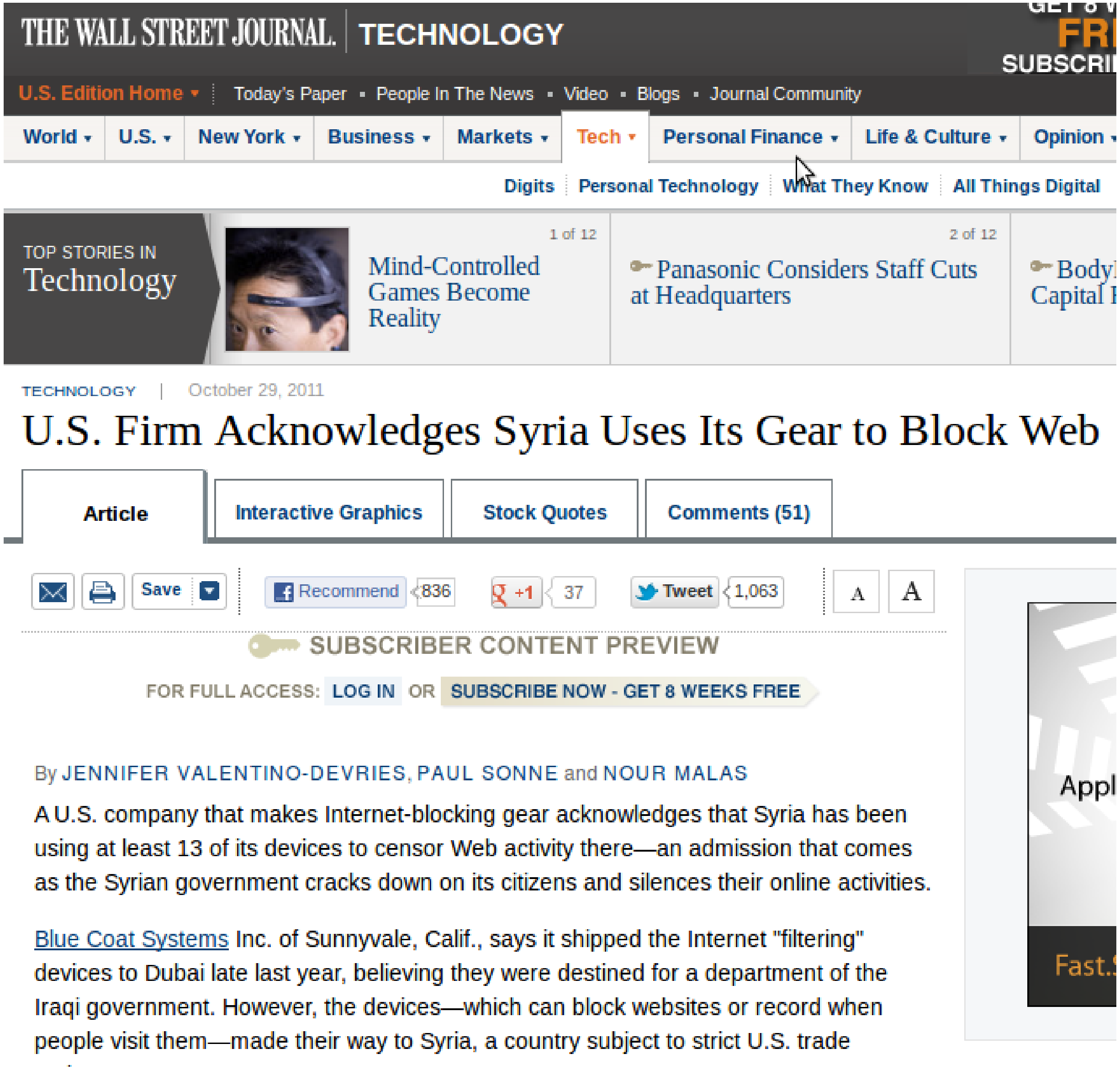
Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes

On Wednesday, EFF will give recommendations to the European Parliament for how to combat one of the most troubling problems facing democracy activists around the world: the fact that European and American companies are providing key surveillance technology to authoritarian governments that is then being used to aid repression.

Recent reports by the *Wall Street Journal* and *Bloomberg News* have exposed the shadowy but growing industry that sells electronic spy gear to governments known for violating human rights. The technology's reach is very broad: governments can listen in on cell phone calls, use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track one's every movement using GPS, and can even *change* email contents while en route to a recipient. Some tools are installed using the same type of malicious malware and spyware used by online criminals to steal credit card

http://en.wikipedia.org/wiki/File:Red-light-camera-springfield-ohio.jpg

Sometimes Transparency Can be Painful...


THE WALL STREET JOURNAL. | TECHNOLOGY
GET 8 W
FR
SUBSCRI
U.S. Edition Home ▾
Today's Paper • People In The News • Video • Blogs • Journal Community
World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life & Culture ▾ | Opinion ▾
Digits | Personal Technology | What They Know | All Things Digital
TOP STORIES IN
Technology
1 of 12
Mind-Controlled Games Become Reality
2 of 12
Panasonic Considers Staff Cuts at Headquarters
Body
Capital I
Article | Interactive Graphics | Stock Quotes | Comments (51)
Save
Recommend 836
+1 37
Tweet 1,063
A A
SUBSCRIBER CONTENT PREVIEW
FOR FULL ACCESS: LOG IN OR SUBSCRIBE NOW - GET 8 WEEKS FREE
Appl
Fast.

TECHNOLOGY | October 29, 2011

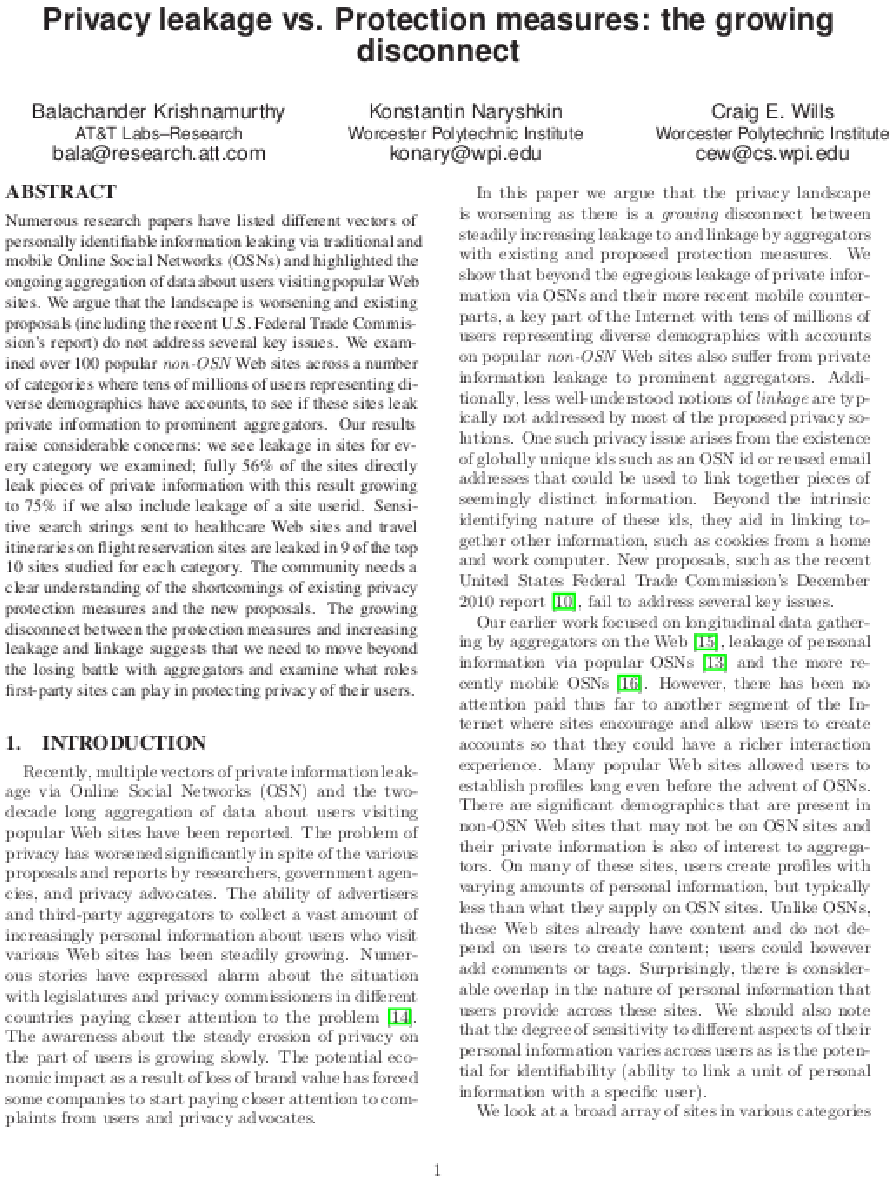
U.S. Firm Acknowledges Syria Uses Its Gear to Block Web

By JENNIFER VALENTINO-DEVRIES, PAUL SONNE and NOUR MALAS

A U.S. company that makes Internet-blocking gear acknowledges that Syria has been using at least 13 of its devices to censor Web activity there—an admission that comes as the Syrian government cracks down on its citizens and silences their online activities.

Blue Coat Systems Inc. of Sunnyvale, Calif., says it shipped the Internet "filtering" devices to Dubai late last year, believing they were destined for a department of the Iraqi government. However, the devices—which can block websites or record when people visit them—made their way to Syria, a country subject to strict U.S. trade

Conduct and Share (Admissible) Research



Privacy leakage vs. Protection measures: the growing disconnect

Balachander Krishnamurthy
AT&T Labs–Research
bala@research.att.com

Konstantin Naryshkin
Worcester Polytechnic Institute
konary@wpi.edu

Craig E. Wills
Worcester Polytechnic Institute
cew@cs.wpi.edu

ABSTRACT

Numerous research papers have listed different vectors of personally identifiable information leaking via traditional and mobile Online Social Networks (OSNs) and highlighted the ongoing aggregation of data about users visiting popular Web sites. We argue that the landscape is worsening and existing proposals (including the recent U.S. Federal Trade Commission's report) do not address several key issues. We examined over 100 popular *non-OSN* Web sites across a number of categories where tens of millions of users representing diverse demographics have accounts, to see if these sites leak private information to prominent aggregators. Our results raise considerable concerns: we see leakage in sites for every category we examined; fully 56% of the sites directly leak pieces of private information with this result growing to 75% if we also include leakage of a site userid. Sensitive search strings sent to healthcare Web sites and travel itineraries on flight reservation sites are leaked in 9 of the top 10 sites studied for each category. The community needs a clear understanding of the shortcomings of existing privacy protection measures and the new proposals. The growing disconnect between the protection measures and increasing leakage and linkage suggests that we need to move beyond the losing battle with aggregators and examine what roles first-party sites can play in protecting privacy of their users.

1. INTRODUCTION

Recently, multiple vectors of private information leakage via Online Social Networks (OSN) and the two-decade long aggregation of data about users visiting popular Web sites have been reported. The problem of privacy has worsened significantly in spite of the various proposals and reports by researchers, government agencies, and privacy advocates. The ability of advertisers and third-party aggregators to collect a vast amount of increasingly personal information about users who visit various Web sites has been steadily growing. Numerous stories have expressed alarm about the situation with legislatures and privacy commissioners in different countries paying closer attention to the problem [14]. The awareness about the steady erosion of privacy on the part of users is growing slowly. The potential economic impact as a result of loss of brand value has forced some companies to start paying closer attention to complaints from users and privacy advocates.

In this paper we argue that the privacy landscape is worsening as there is a *growing* disconnect between steadily increasing leakage to and linkage by aggregators with existing and proposed protection measures. We show that beyond the egregious leakage of private information via OSNs and their more recent mobile counterparts, a key part of the Internet with tens of millions of users representing diverse demographics with accounts on popular *non-OSN* Web sites also suffer from private information leakage to prominent aggregators. Additionally, less well-understood notions of *linkage* are typically not addressed by most of the proposed privacy solutions. One such privacy issue arises from the existence of globally unique ids such as an OSN id or reused email addresses that could be used to link together pieces of seemingly distinct information. Beyond the intrinsic identifying nature of these ids, they aid in linking together other information, such as cookies from a home and work computer. New proposals, such as the recent United States Federal Trade Commission's December 2010 report [10], fail to address several key issues.

Our earlier work focused on longitudinal data gathering by aggregators on the Web [15], leakage of personal information via popular OSNs [13] and the more recently mobile OSNs [16]. However, there has been no attention paid thus far to another segment of the Internet where sites encourage and allow users to create accounts so that they could have a richer interaction experience. Many popular Web sites allowed users to establish profiles long even before the advent of OSNs. There are significant demographics that are present in non-OSN Web sites that may not be on OSN sites and their private information is also of interest to aggregators. On many of these sites, users create profiles with varying amounts of personal information, but typically less than what they supply on OSN sites. Unlike OSNs, these Web sites already have content and do not depend on users to create content; users could however add comments or tags. Surprisingly, there is considerable overlap in the nature of personal information that users provide across these sites. We should also note that the degree of sensitivity to different aspects of their personal information varies across users as is the potential for identifiability (ability to link a unit of personal information with a specific user).

We look at a broad array of sites in various categories

ACM Computers Freedom and Privacy

Workshop on Privacy in the Electronic Society (WPES)

Privacy Enhancing Technologies Symposium (PETS)

... and don't forget Legal, Government, Military, and Industry events

Don't Forget Executive Summary Versions too...

Take it to Congress

TSA Oversight: Effective Security or Security Theater
House Oversight Committee
(26 March 2012)

The work of our two Committees has documented a recurring pattern of mismanagement and waste at the Transportation Security Administration.

Add to this an unending string of video clips, photographs and news reports about inappropriate, clumsy and even illogical searches and screenings by TSA agents...

http://oversight.house.gov/hearing/tsa-oversight-part-iii-effective-security-or-security-theater/

Take it to Court

FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling

http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/

Take it to the White House

White House “Privacy Bill of Rights”

http://www.wired.com/threatlevel/2012/02/privacy-bill-of-rights/

Some Have Chosen More Extreme Measures

Non-Violent Civil Disobedience

Principality of Sealand

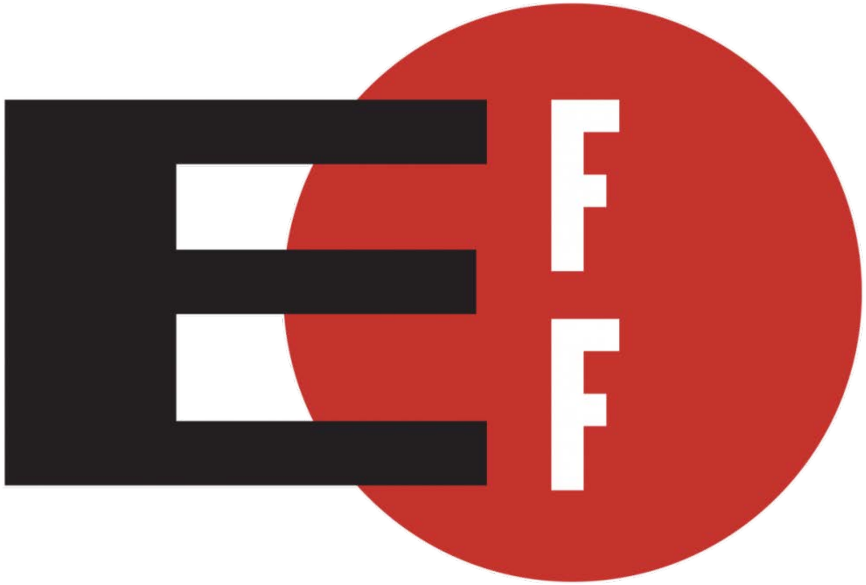
Hactivism

Formation of the Pirate Party

Tahrir Square, Egypt
8 February 2011

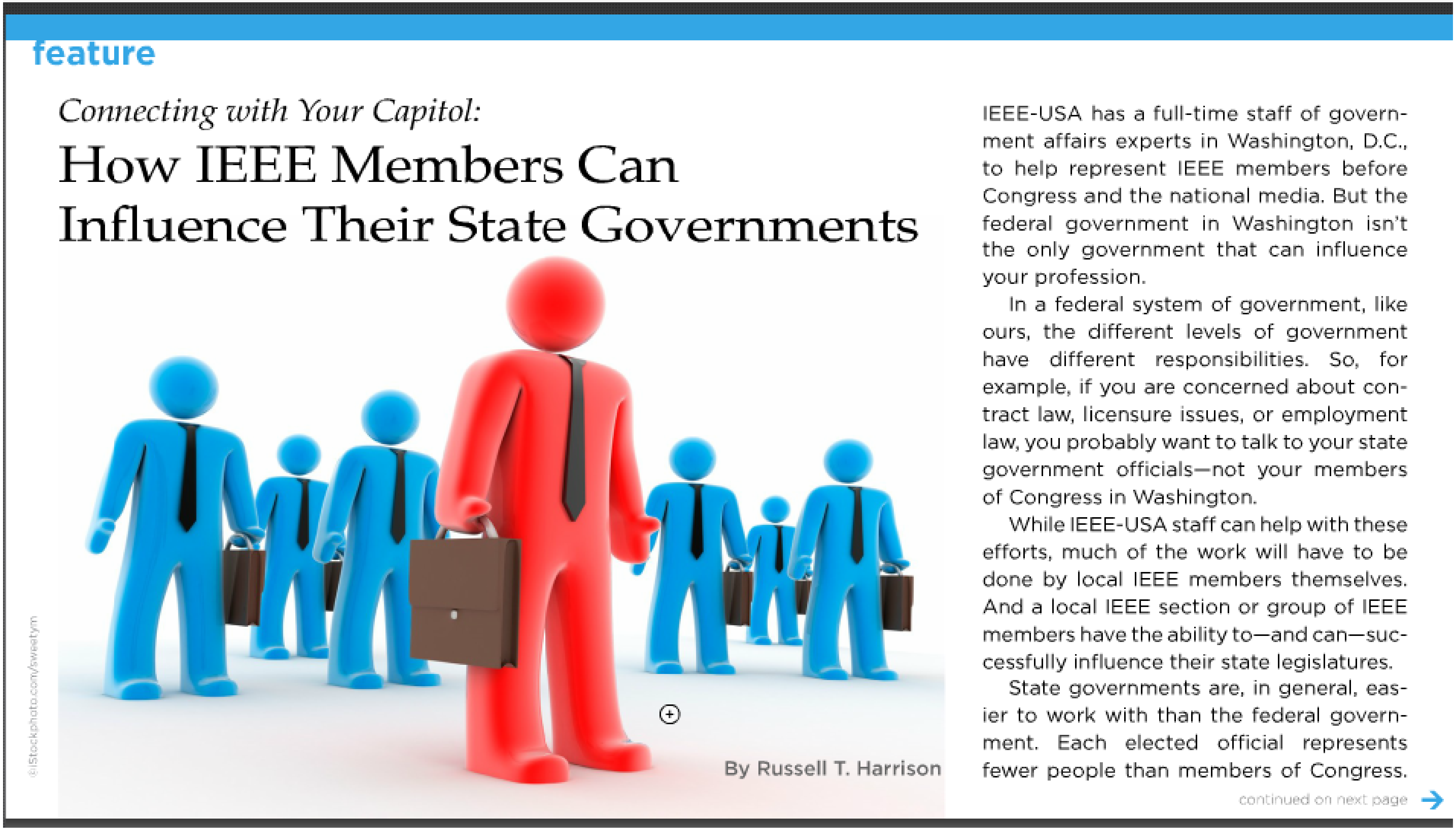
http://www.sealandgov.org/
http://www.komonews.com/news/local/KATU-147866735.html
http://en.wikipedia.org/wiki/File:Tahrir_Square_during_8_February_2011.jpg
http://en.wikipedia.org/wiki/File:Anonymous_at_Scientology_in_Los_Angeles.jpg
http://yro.slashdot.org/story/12/05/07/015212/pirate-party-gaining-strength-in-germany

Support Your Privacy Champions of Choice



http://www.wired.com/threatlevel/2012/02/privacy-bill-of-rights/

Join a Professional Society



feature

Connecting with Your Capitol:

How IEEE Members Can Influence Their State Governments

By Russell T. Harrison

©iStockphoto.com/sweetym

IEEE-USA has a full-time staff of government affairs experts in Washington, D.C., to help represent IEEE members before Congress and the national media. But the federal government in Washington isn't the only government that can influence your profession.

In a federal system of government, like ours, the different levels of government have different responsibilities. So, for example, if you are concerned about contract law, licensure issues, or employment law, you probably want to talk to your state government officials—not your members of Congress in Washington.

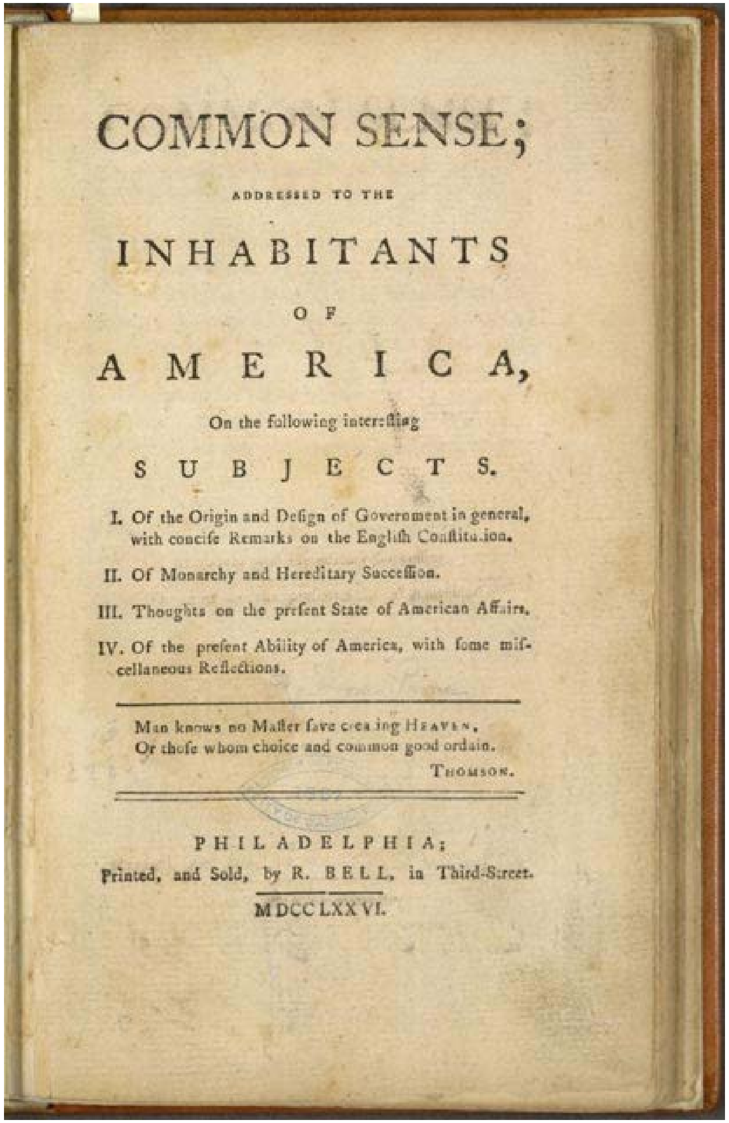
While IEEE-USA staff can help with these efforts, much of the work will have to be done by local IEEE members themselves. And a local IEEE section or group of IEEE members have the ability to—and can—successfully influence their state legislatures.

State governments are, in general, easier to work with than the federal government. Each elected official represents fewer people than members of Congress.

continued on next page →

http://www.nxtbook.com/nxtbooks/ieeeusa/ieeeusa_summer12/index.php#/10

Common Sense



COMMON SENSE;

ADDRESSED TO THE

INHABITANTS

OF

AMERICA,

On the following intereſting

SUBJECTS.

I. Of the Origin and Deſign of Government in general, with conciſe Remarks on the Engliſh Conſtitution.

II. Of Monarchy and Hereditary Succeſſion.

III. Thoughts on the preſent State of American Affairs.

IV. Of the preſent Ability of America, with ſome miſcellaneous Reflections.

Man knows no Maſter ſave creating HEAVEN,
Or thoſe whom choice and common good ordain.
THOMSON.

PHILADELPHIA;
Printed, and Sold, by R. BELL, in Third-Street.
MDCCLXXVI.

http://en.wikipedia.org/wiki/Common_Sense_%28pamphlet%29

Parting Thoughts...

Lumbering Bureaucracy

http://lotr.wikia.com/wiki/Ents

Beware Counter-Counter Measures

Miami Beach Police Ordered Videographer at Gunpoint to Hand Over Phone

http://www.pixiq.com/article/video-showing-mb-cops-pointing-gun-at-man-for-recording-them
http://www.pixiq.com/article/MIami%20Beach%20Police%20Ordered%20Videographer%20At%20Gunpoint%20To%20Hand%20Over

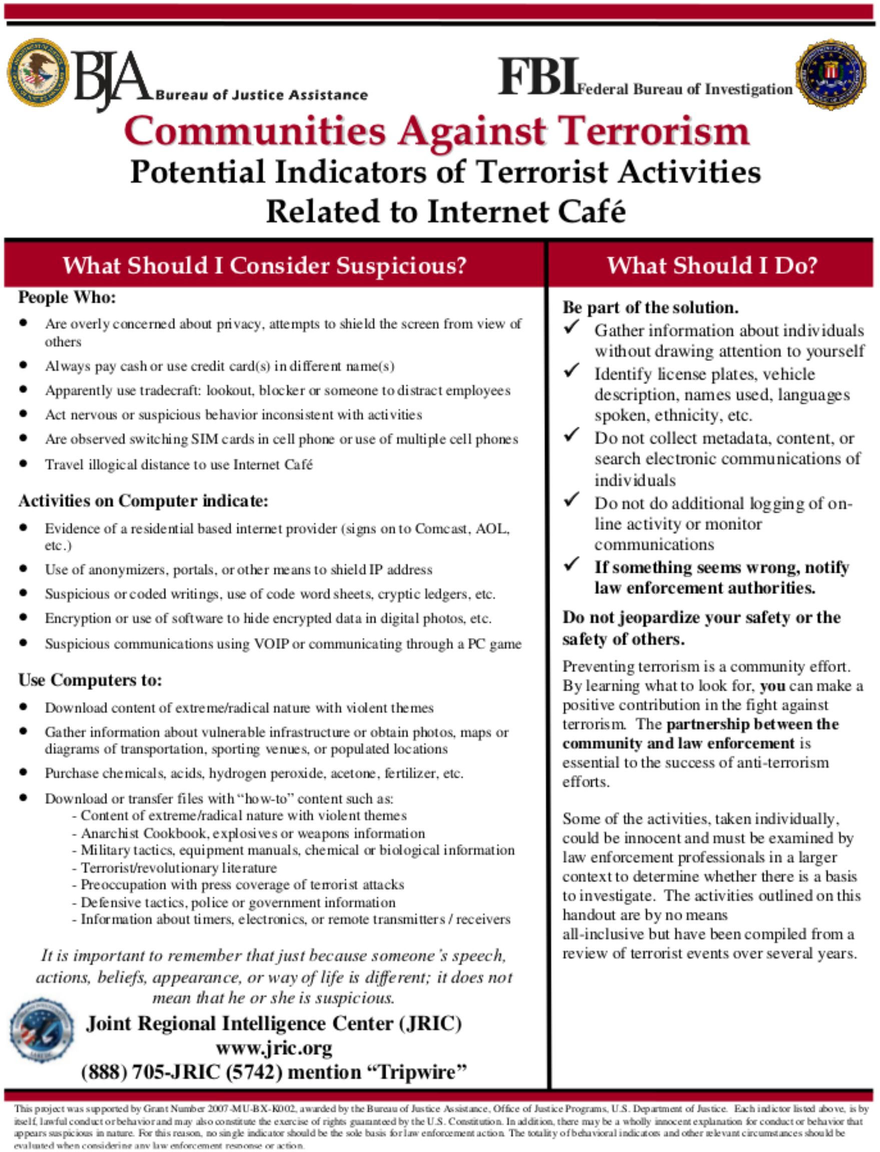
Don't be put off by Naysayers...

The introduction sounds more like a political manifesto than a piece of security research.

It is filled with inappropriate and sensational speculation (e.g., "Today's 'free' societies may slide toward a police state through Pearl Harbor-like events and totalitarian governments may rise to power. Consider [DARPA's] Total Information Awareness program...").

Before making such baseless assessments and implications, consider that people who work for DARPA and the U.S. government do participate in program committees.

Well Intentioned, but...



BJA Bureau of Justice Assistance

FBI Federal Bureau of Investigation

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to Internet Café

What Should I Consider Suspicious?

People Who:

- Are overly concerned about privacy, attempts to shield the screen from view of others
- Always pay cash or use credit card(s) in different name(s)
- Apparently use tradecraft: lookout, blocker or someone to distract employees
- Act nervous or suspicious behavior inconsistent with activities
- Are observed switching SIM cards in cell phone or use of multiple cell phones
- Travel illogical distance to use Internet Café

Activities on Computer indicate:

- Evidence of a residential based internet provider (signs on to Comcast, AOL, etc.)
- Use of anonymizers, portals, or other means to shield IP address
- Suspicious or coded writings, use of code word sheets, cryptic ledgers, etc.
- Encryption or use of software to hide encrypted data in digital photos, etc.
- Suspicious communications using VOIP or communicating through a PC game

Use Computers to:

- Download content of extreme/radical nature with violent themes
- Gather information about vulnerable infrastructure or obtain photos, maps or diagrams of transportation, sporting venues, or populated locations
- Purchase chemicals, acids, hydrogen peroxide, acetone, fertilizer, etc.
- Download or transfer files with "how-to" content such as:
  - Content of extreme/radical nature with violent themes
  - Anarchist Cookbook, explosives or weapons information
  - Military tactics, equipment manuals, chemical or biological information
  - Terrorist/revolutionary literature
  - Preoccupation with press coverage of terrorist attacks
  - Defensive tactics, police or government information
  - Information about timers, electronics, or remote transmitters / receivers

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.

Joint Regional Intelligence Center (JRIC)
www.jric.org
(888) 705-JRIC (5742) mention "Tripwire"

What Should I Do?

Be part of the solution.

- ✓ Gather information about individuals without drawing attention to yourself
- ✓ Identify license plates, vehicle description, names used, languages spoken, ethnicity, etc.
- ✓ Do not collect metadata, content, or search electronic communications of individuals
- ✓ Do not do additional logging of on-line activity or monitor communications
- ✓ **If something seems wrong, notify law enforcement authorities.**

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Each indictor listed above, is by itself, lawful conduct or behavior and may also constitute the exercise of rights guaranteed by the U.S. Constitution. In addition, there may be a wholly innocent explanation for conduct or behavior that appears suspicious in nature. For this reason, no single indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

<u>Suspicious Activities</u>

"Overly concerned about privacy"

"Always pays cash"

"Use of anonymizers...

to shield IP address"

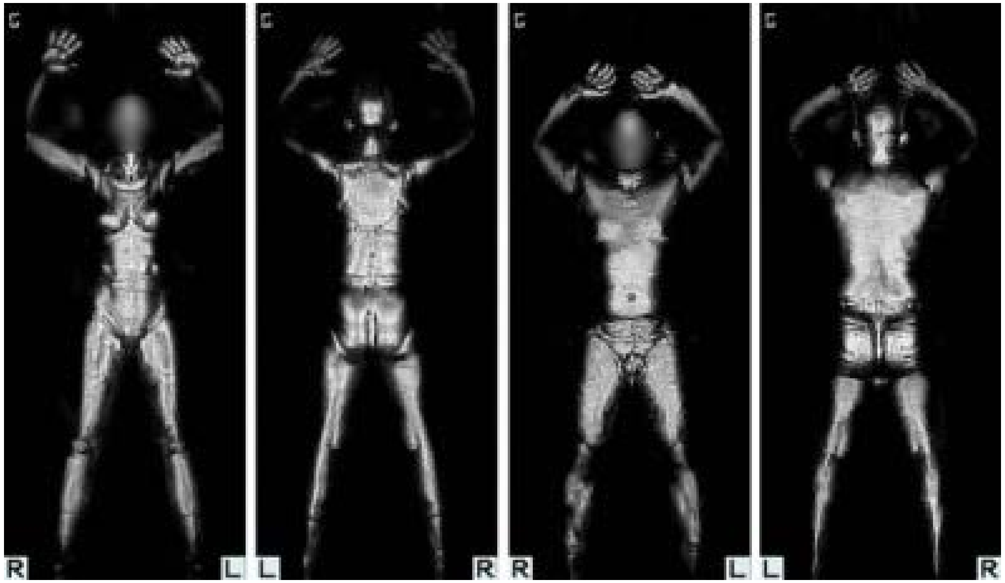
"Uses encryption"

"Downloads information

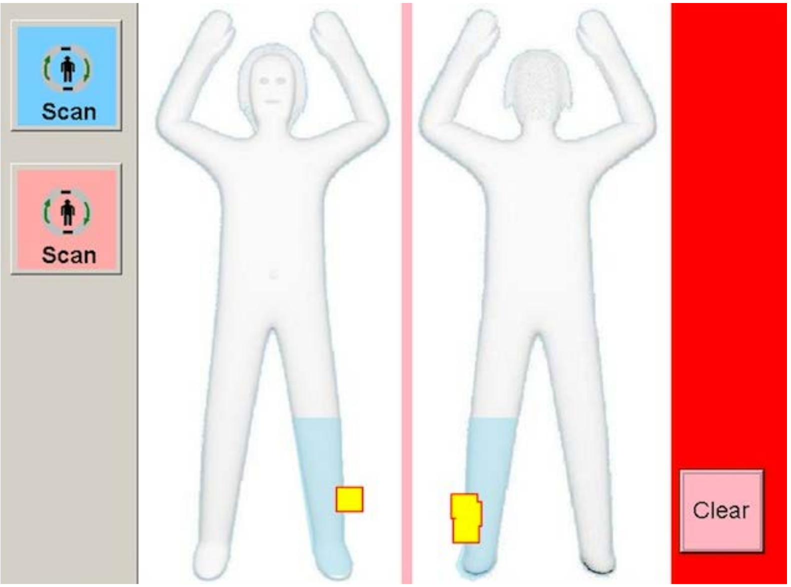
about electronics"

http://yro.slashdot.org/story/12/02/02/1719221/do-you-like-online-privacy-you-may-be-a-terrorist

Seek Actionable Changes



Before

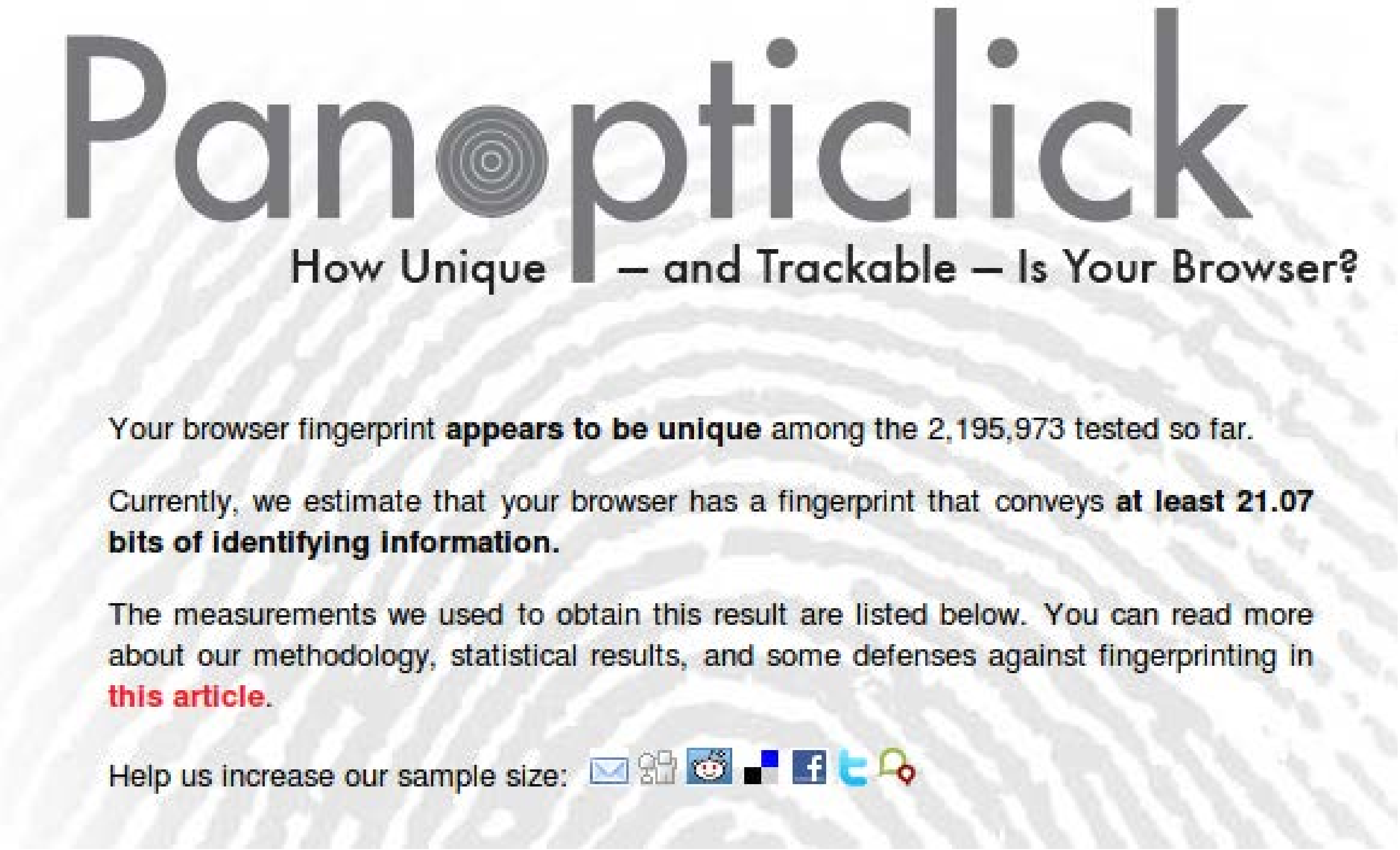


After

See also Opt-In, Anonymization, Accountability, Consent, Limited Collection, Limited Use, Disclosure and Retention, Accuracy, Safeguards, Individual Access, Ability to Challenge, Privacy by Design...

http://www.wired.com/threatlevel/2011/07/ts/
Simson Garfinkel, "Canadian Standards Association Code for Protecting Personal Information," Database Nation, p279

Risk of Uniqueness



Your browser fingerprint **appears to be unique** among the 2,195,973 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.07 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

See Peter Eckersley's "How Unique is Your Browser?" from Defcon 18
and https://panopticlick.eff.org/

In Conclusion…

- Networked surveillance systems threaten our privacy and our free way of life
- Individuals can and should protect themselves
- This community has the knowledge and status to deflect the trajectory of our surveilled future

For More Information...

Lisa Shay, Dominic Larkin, John Nelson, and Gregory Conti. "A Framework for Analysis of Quotidian Exposure in an Instrumented World." to be presented at IEEE International Carnahan Conference on Security Technology, October 2012.

Greg Conti, Lisa Shay, and Woody Hartzog. "Life Inside a Skinner Box: Confronting our Future of Automated Law Enforcement." DEFCON 20, July 2012.

Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin and Gregory Conti. "Confronting Automated Law Enforcement." We Robot, April 2012.

Greg Conti. "Our Instrumented Lives: Sensors, Sensors, Everywhere." DEFCON 18, July 2010.

We'd also like to thank John Nelson, Woody Hartzog, and Dominic Larkin for their support of this work.

Questions?

http://commons.wikimedia.org/wiki/File:Lamp_surveillance_cameras.jpg