CSE331 Computer Security Fundamentals

11/30/2017 **Privacy**

Michalis Polychronakis

Stony Brook University

Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Real-world Privacy

Large-scale data collection examples

- Credit cards, Metrocards, loyalty cards
- Street/public space cameras
- E-ZPass
- Named tickets
- …

Part of our everyday activities and personal information is (voluntarily or compulsorily) recorded

- Information from different sources can be **correlated**
- *Did you buy your Metrocard with your credit card?*

The same happens in the online world…

Third parties have access to…

Our email (Gmail, Yahoo, …)

Our files (Dropbox, Google Drive, …)

Our finances (e-banking, credit reporting, Mint, …)

Our communication (Skype, Facebook, …)

Our traffic (WiFi hotspots, ISPs, …)

Our location (3/4G, GPS, WiFi, …)

Our activities (browsing history, daily routine, …)

Our preferences ("Likes," Amazon, Netflix, …)

Our health (Fitbit, iWatch, 23andMe, …)

…

BUSINESS DAY

Millions of Anthem Customers Targeted in Cyberattack

By REED ABELSON and MATTHEW GOLDSTEIN FEB. 5, 2015

Outside the Anthem facility in Indianapolis. Anthem said it detected a data breach on Jan. 29, and that it was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images

Anthem, one of the nation's largest health insurers, said late

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

Email

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than

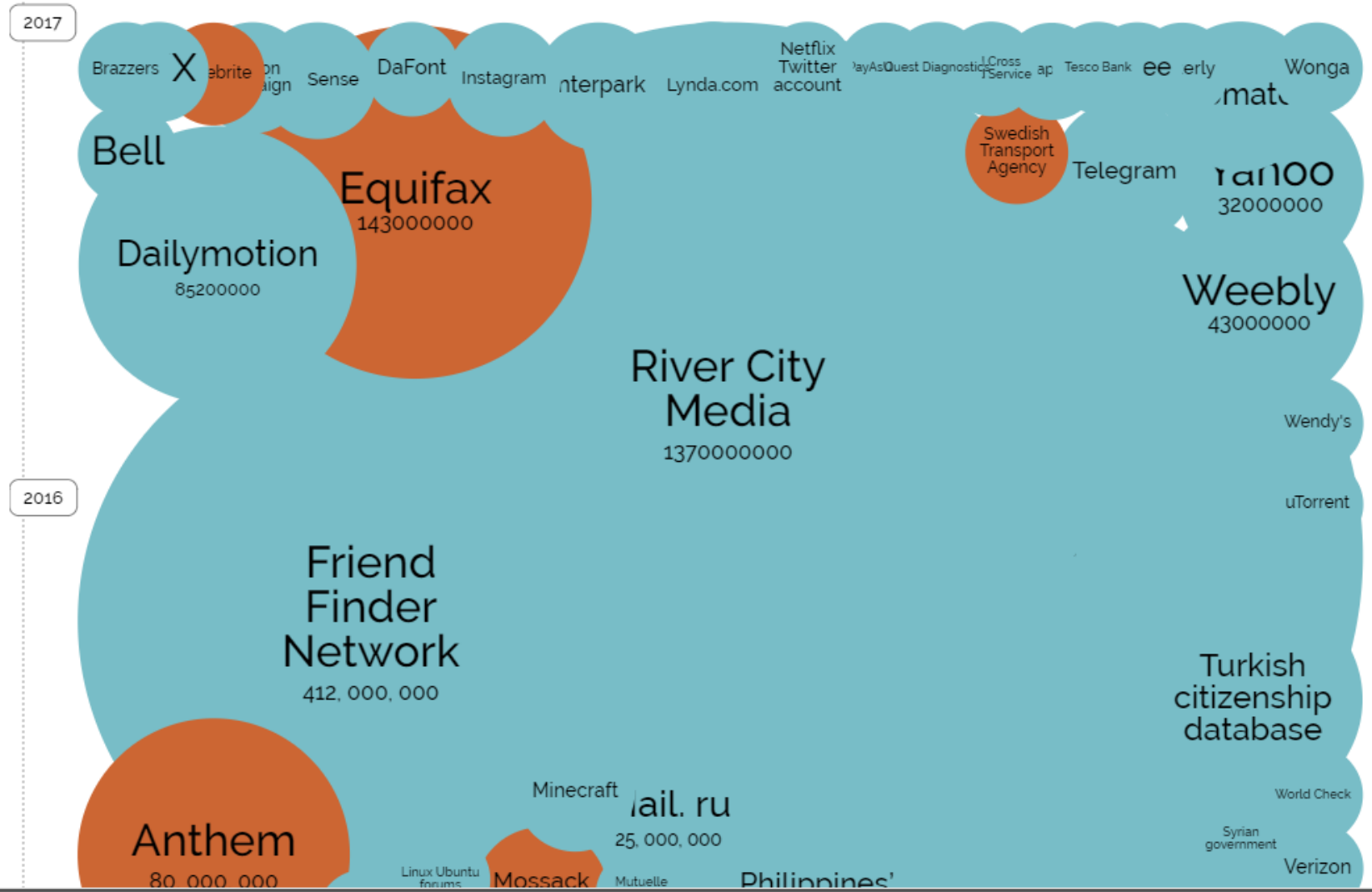
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)

interesting story

YEAR | BUBBLE COLOUR: YEAR | METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



Egham, U.K., February 7, 2017

View All Press Releases

Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016

Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017

Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

Regionally, Greater China, North America and Western Europe are driving the use of connected things and the three regions together will represent 67 percent of the overall Internet of Things (IoT) installed base in 2017.

Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017

The consumer segment is the largest user of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use (see Table 1). Businesses are on pace to employ 3.1 billion connected things in 2017. "Aside from automotive systems, the applications that will be most in use by consumers will be smart TVs and digital set-top boxes, while smart electric meters and commercial security cameras will be most in use

How A Coffee Machine Infected Factory Computers with Ransomware

By Waqas on July 28, 2017 Email @hackread CYBER ATTACKS HACKING NEWS MALWARE SECURITY

It's no surprise that the Internet of Things (IoT) devices are highly vulnerable to cyber attacks but who would know a time would come when these devices will become a security threat to institutions?

A few months ago researchers exposed life threatening vulnerabilities in IIoT (Industrial Internet of Things) devices specifically Industrial robots. In their findings, robots could be hacked, but in this case, we are about to discuss a smart coffee machine or an Internet connected coffee machine.

More: San Francisco Railway' Fare System Hacked for 100 Bitcoin Ransom

The incident took place in June 2017 and was shared by a chemical engineer on Reddit who goes by the handle of "C10H15N1." He works as a PLC (Programmable Logic Controllers) expert in a company that has multiple petrochemical factories making chemicals in Europe.

Innovations

How a fish tank helped hack a casino

By Alex Schiffer July 21

Hackers stole data from a casino by hacking into an Internet-connected fish tank, according to a new report. (iStock)


New Rules in China Upset Western Tech Companies

STATE OF THE ART
Uber's Business Model Could Change Your Work


ECONOMIC SCENE
Job Licenses in Spotlight as Uber Rises


DEALBOOK
After Alibaba Spinoff, Yahoo May Become a Takeover Target

Bits

SECURITY

Apple Says It Will Add New iCloud Security Measures After Celebrity Hack

By BRIAN X. CHEN SEPTEMBER 4, 2014 11:32 PM 21 Comments

PREVIOUS POST
Microsoft Introduces Three New Smartphones

NEXT POST
Daily Report: Apple Expected to Unveil Smartwatch and Larger iPhones

SCUTTLEBOT *News from the Web, annotated by our staff*

Netflix's Secret Special Algorithm Is a Human
NEW YORKER | His name, writes Tim Wu, is Ted Sarandos. - *Natasha Singer*

Uber Releases Study on Drunk Driving and Transportation
UBER BLOG | A new study released by the ride-hailing company claims it is having a "measurable impact on driving down alcohol-related crashes." - *Mike Isaac*

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

But the deeper aspects of your personality remain hard to detect.

MORE IN TECHNOLOGY

Introducing the Supertweet
IAN BOGOST

My Parents' Facebook Will
JAKE SWEARINGEN

Facebook knows you're gay before you do

3/20/13 4:29pm by Jon Green 39 Comments

Am I the only one creeped out that Facebook is now guessing, sometimes correctly, if its users are gay?

In the world of Big Data, our private lives are increasingly becoming intermingled with the shadowy, yet public, world of cyberspace.

Whenever we go online we are providing data that can be used to market to us; from Google searches to Facebook likes to eBay purchases, we are inputting data into a series of mathematical models which make *incredibly* educated guesses about the kinds of people we are.

Facebook creepily offers help to a gay guy thinking of "coming out"

Enter Matt. As BuzzFeed notes, Matt was your typical Facebook user who suddenly found an ad in his news feed for help in coming out. The weird thing was that Matt "did" need help coming out, and understandably he was more than a bit curious as to how Facebook knew.

At first, Matt wondered if Facebook had accessed his text messages, as he had confided in a close friend the previous

LATEST COMMENTS TAGS

Let's slow down this race, together: Starbuc and a bad hashtag
3/20/15 12:00pm 7 Comments

It's time to make college free
3/20/15 10:00am 19 Comments

Rick Perry's new adviser has suggested tha God isn't #ReadyForHillary. Technically, he right.
3/20/15 8:00am 14 Comments

Fatwas, gay sex tourism and the Indonesian LGBT underground
3/19/15 10:00am 6 Comments

Support AMERICAblog

Click here to donate securely via PayPal

We Recommend

Parallels between India's sexism and America's racism

Facebook

Facebook users unwittingly revealing intimate secrets, study finds

Personal information including sexuality and drug use can be correctly inferred from public 'like' updates, according to study

Most popular in US


Barcelona v Real Madrid: El Clásico – live! Jacob Steinberg


The eight best young adult books – and why grownups should read them, too


Singapore's Lee Kuan Yew dies aged 91

TECH 2/16/2012 @ 11:02AM | 2,698,356 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and

Web Browsing Tracking

Webpages are often mashups of content loaded from different sources

- Ads, images, videos, widgets, …
- IMG URLs, IFRAMEs, JavaScript, web fonts, Flash/applets, …
- Hosted on third-party servers: CDNs, cloud providers, ad networks, …

A third party involved in many different websites can track user visits across all those websites

- 2+ third parties may collude to expand their collective "view"

Need to learn two key pieces of information

- ***What webpage was visited***
- ***Who visited it***

Microsoft Announces Con

techcrunch.com/2015/04/29/microsoft-announces-continuum-turning-windows-10-phones-into-desktop

68

News Startups

Apps Microsoft Windows

Microsoft An... Phones Into...

Posted 2 hours ago by Kyle ...

1,769 SHARES

DISCONNECT

Show list view

Browse the web normally. As you do, the graph in this popup and the counter in the toolbar will update. Each circle in the graph represents a site that's been or would've been sent some of your personal info.

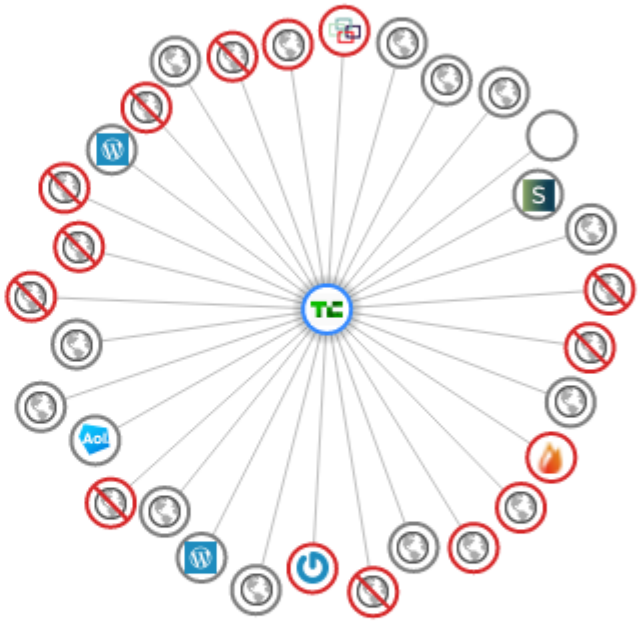
Circles with a halo are sites you've visited. Circles without a halo are sites you haven't.

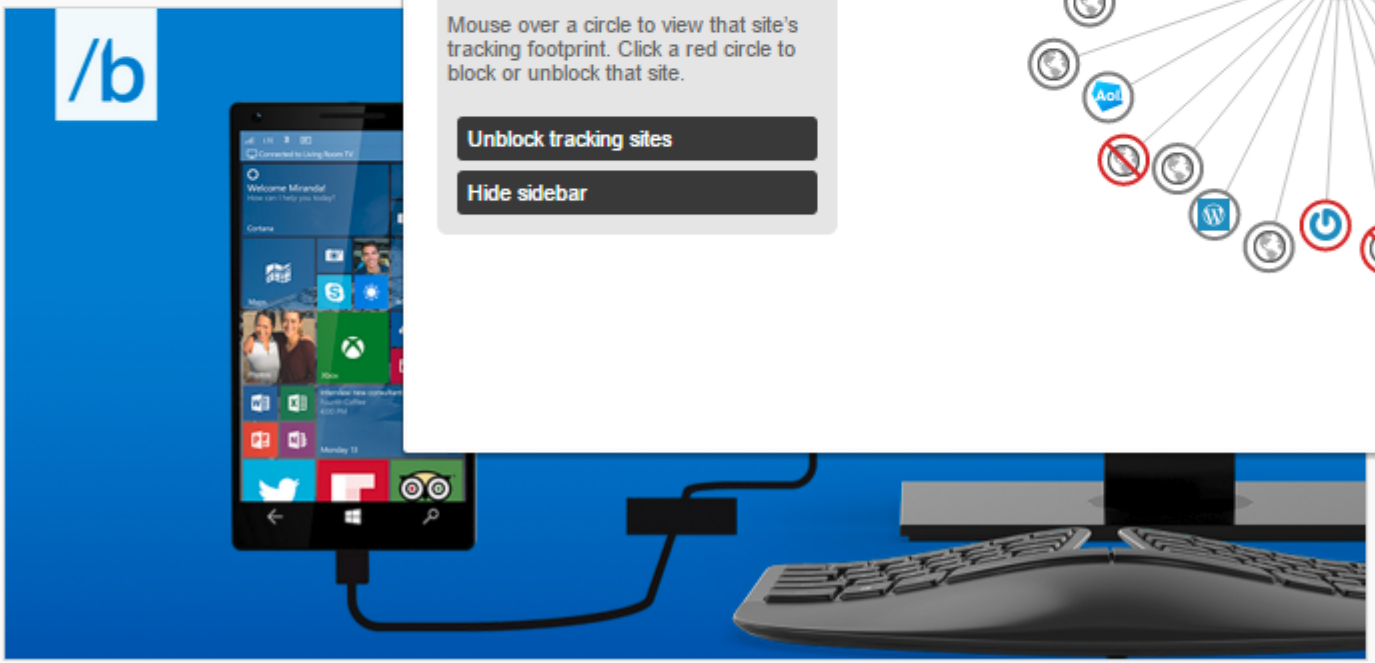
Red circles are known tracking sites. Gray circles aren't but may still track you.

Mouse over a circle to view that site's tracking footprint. Click a red circle to block or unblock that site.

Unblock tracking sites

Hide sidebar





Microsoft just demonstrated one of the intriguing possibilities from its single platform/multiple

What webpage was visited?

HTTP Referer [sic] header

- The URL of the webpage from which a link was followed
- Useful for statistics/analytics, bad for privacy
- Can be turned off trough browser options/extensions
- HTML5 rel="noreferrer" anchor attribute to indicate to the user agent not to send a referrer when following the link

Page-specific, session-specific, user-specific URLs

- Unique URL per page (even for the same resource) ➔ track what page was visited
- Unique URL per session/user ➔ distinguish between visits from different users

Tracking URLs are also commonly used in promotional emails

Embedded image loading

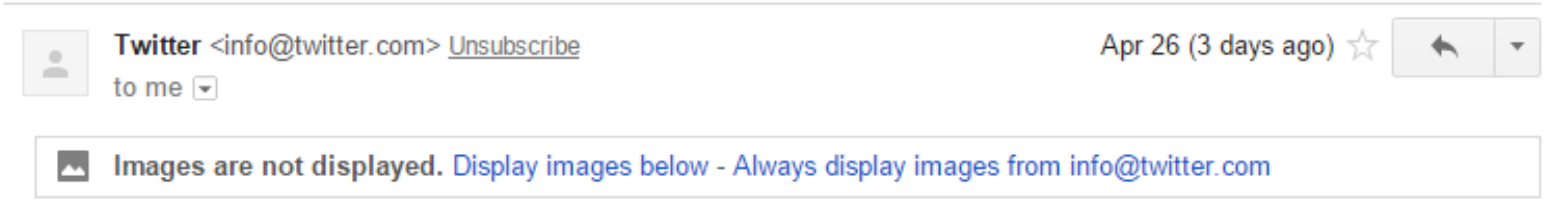
- This is an active email address!
- Detect the time a user viewed a message
- The request reveals much more: user agent, device, location, …

Embedded links

- Learn which email addresses resulted in visits (click-through rate)

Default behavior of email clients varies

- Gmail used to block images by default, now uses image proxy servers
- Tracking through unique images still possible: senders can track the first time a message is opened (user's IP is not exposed though)



Who visited the page?

Browsing to a web page reveals a wealth of information

Source IP address

- Not very accurate (e.g., NAT, DHCP, on-the-go users) but still useful

Third-party cookies: precise user tracking

- Easy to block (configurable in most browsers, defaults vary)

"Evercookies:" exploit alternative browser state mechanisms

- Flash/Silverlight/other plugin-specific storage, ETags, HTML5 session/logal/global storage, caches, …

Browser/device fingerprinting: recognize unique system characteristics

- Browser user agent, capabilities, plugins, system fonts, screen resolution, time zone, and numerous other properties

What do web tracking techniques really track?

Distinguish between different visitors

Track anonymous individuals

Actually: track the pages visited by a particular browser running on a particular device

Better: distinguish between different *persons*

Track named individuals

The transition is easy…

Personally identifiable information (PII) is often voluntarily provided to websites:

Social networks, cloud services, web sites requiring user registration, …

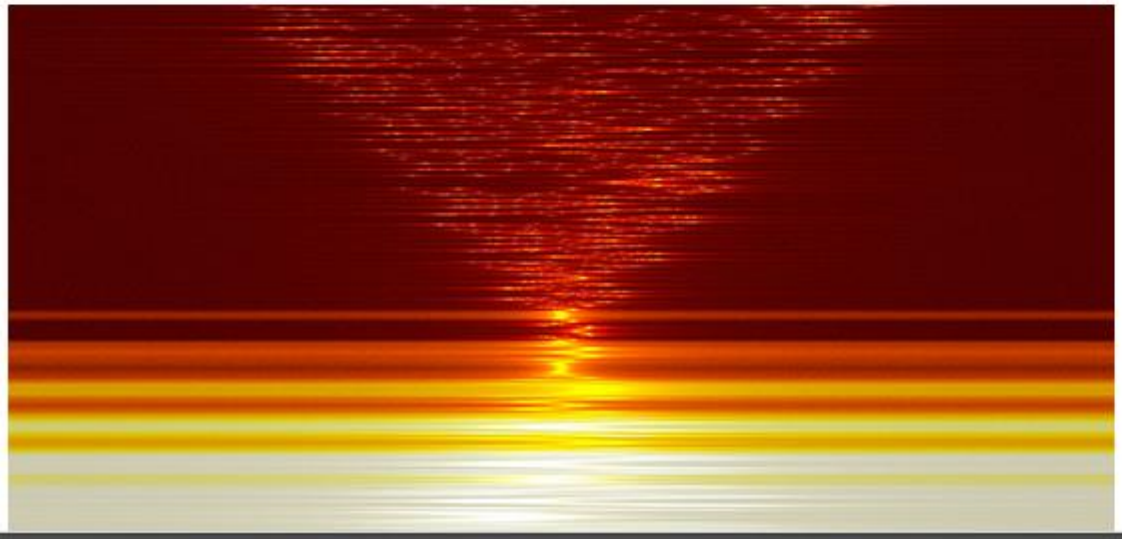
Cookies/sessions are associated with PII

Contamination: trackers may collude with services

Previously "anonymous" cookies/fingerprints can be associated with named individuals

ROBERT MCMILLAN 10.27.14 6:30 AM

VERIZON'S 'PERMA-COOKIE' IS A PRIVACY-KILLING MACHINE



LATEST NEWS

JAKOB SCHILLER
Stunning Snowy Landscapes from the Edge of the Earth
3 MINS

SPACE
Jeff Bezos' Blue Origin Just Launched Its Flagship Rocket
14 MINS

SCIENCE
An Atlas of the Bacteria and Fungi We Breathe Every Day
1 HOUR

DESIGN
The Age of Drone

AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing

AT&T goes head to head against Google in KC on fiber and targeted ads.

by Jon Brodkin - Feb 16, 2015 12:38pm EST

AT&T

AT&T's gigabit fiber-to-the-home service has just arrived in Kansas City, and the price is the same as Google Fiber—if you let AT&T track your Web browsing history.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.

WATCH ARS VIDEO

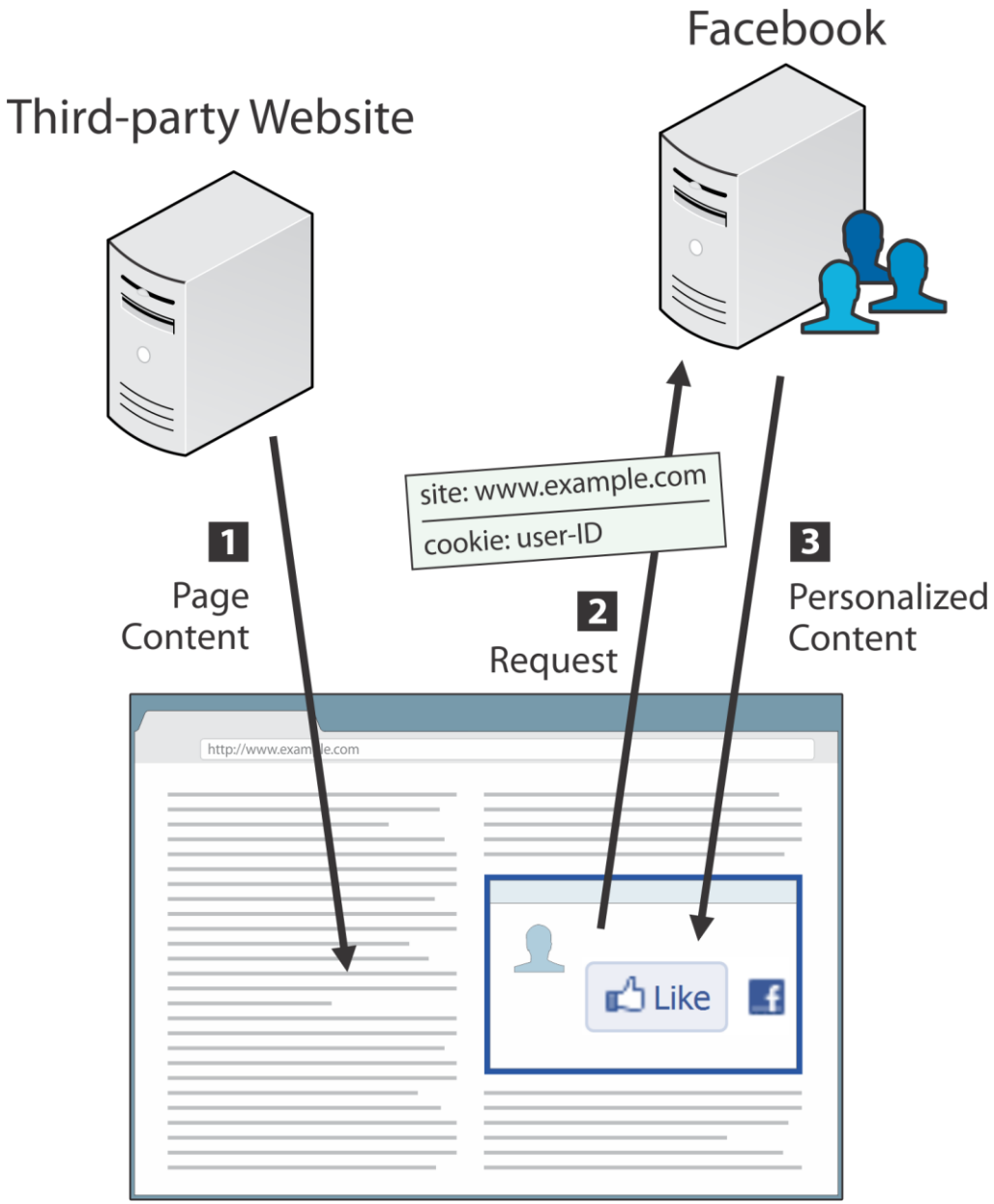
Users register on trackers!

Social plugins are prevalent

- 2+ billion Facebook users
- 33% of the top 10K websites have Like Buttons
- Twitter, Google+, LinkedIn, Pinterest, AddThis, …
- OS/app integration

A growing part of our browsing history can be tracked by social networking services

- Not as merely anonymous visitors, but as ***named persons***
- Just visiting the page is enough (no interaction needed)
- Cross-device tracking


Facebook
Third-party Website
site: www.example.com
cookie: user-ID
1
Page Content
2
Request
3
Personalized Content
http://www.example.com
Like

Existing Solutions

Log out

- Some cookies persist

Block third-party cookies

- Not always effective

Block social widgets completely

Incognito mode

All existing solutions disable content personalization

- Privacy vs. functionality dilemma

(a) Like 43 likes. Sign Up to see what your friends like.

(b) Like 43 people like this.

(c) Like Jane Doe, John Doe and 41 others like this.

First Party Isolation (Firefox)

AKA Cross-Origin Identifier Unlinkability (Tor Browser)

All identifier sources and browser state are scoped (isolated) using the URL bar domain

- Cookies, cache, HTTP Authentication, DOM Storage, Flash cookies, SSL and TLS session resumption, HSTS and HPKP supercookies, OCSP, …

Example: `tracker.com` sets/reads cookies in `bbc.com` and `cnn.com`

- Before: `tracker.com` can track the same person on both sites
- After: `tracker.com` will see two different cookies
- Third party cookies are stored with a tag of the first party (e.g., `bbc.com.tracker.com` and `cnn.com.tracker.com`)

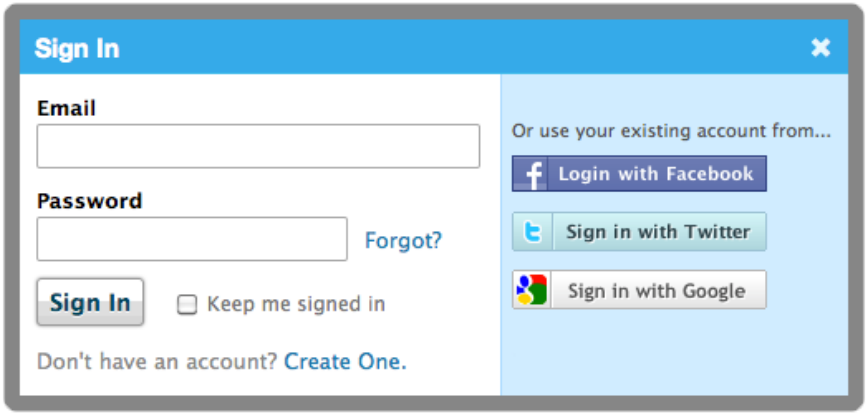
Single Sign-on/Social Login

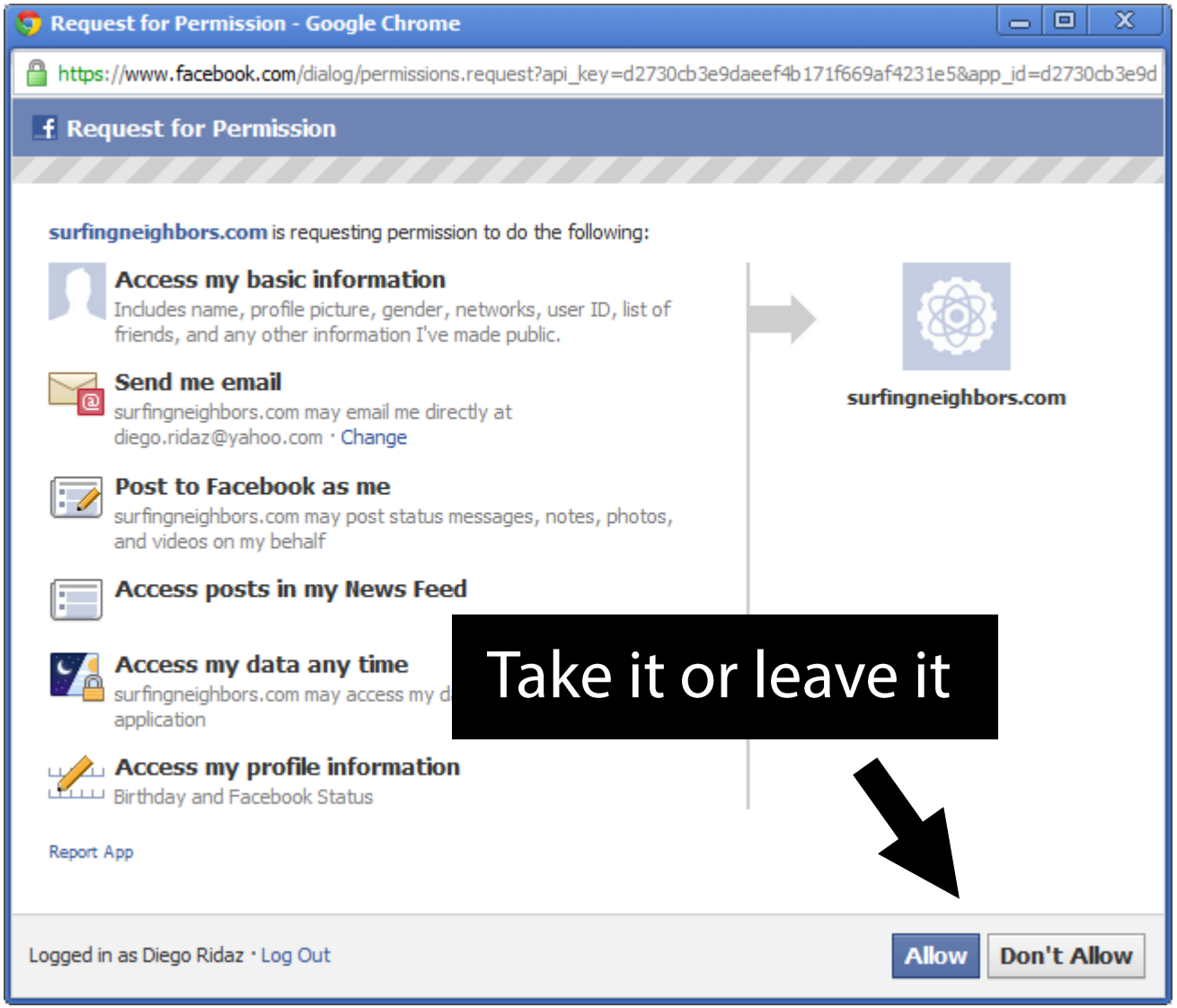
Pros

- Convenience – fewer passwords to remember
- Rich experience through social features
- Outsource user registration and management

Cons

- Same credentials for multiple sites
- User tracking
- Access to user's profile




Request for Permission - Google Chrome
https://www.facebook.com/dialog/permissions.request?api_key=d2730cb3e9daeef4b171f669af4231e5&app_id=d2730cb3e9d
Request for Permission
surfingneighbors.com is requesting permission to do the following:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.
Send me email
surfingneighbors.com may email me directly at diego.ridaz@yahoo.com · Change
Post to Facebook as me
surfingneighbors.com may post status messages, notes, photos, and videos on my behalf
Access posts in my News Feed
Access my data any time
application
Access my profile information
Birthday and Facebook Status
Report App
surfingneighbors.com
Take it or leave it
Logged in as Diego Ridaz · Log Out
Allow
Don't Allow

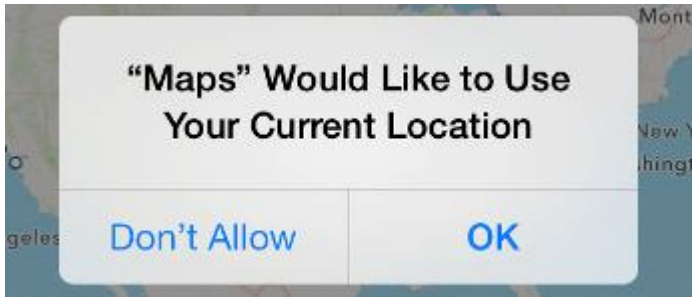
Location Tracking

IP addresses reveal approximate location information

- MaxMind statistics: 99.8% accurate on a country level, 90% accurate on a state level in the US, and 81% accurate for cities in the US within a 50 kilometer radius

Mobile devices allow for precise location tracking

- Cell tower triangulation/trilateration
- GPS, GLONASS, …
- WiFi access points in known locations



Per-app permissions

- Android vs. iOS:
  installation vs. usage time

The New York Times

BUSINESS DAY

410 COMMENTS

Attention, Shoppers: Store Is Tracking Your Cell

By STEPHANIE CLIFFORD and QUENTIN HARDY JULY 14, 2013

Like dozens of other brick-and-mortar retailers, Nordstrom wanted to learn more about its customers — how many came through the doors, how many were repeat visitors — the kind of information that e-commerce sites like Amazon have in spades. So last fall the company started testing new technology that allowed it to track customers' movements by following the Wi-Fi signals from their smartphones.

Brick-and-mortar stores are looking for a chance to catch up with their online competitors by using software that allows them to watch customers as they shop, and gather data about their behavior. Video by Erica Berenstein on July 14, 2013.

But when Nordstrom posted a sign telling customers it was tracking them, shoppers were unnerved.

"We did hear some complaints," said Tara Darrow, a spokeswoman for the store. Nordstrom ended the experiment in May, she said, in part because of the comments.

Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn

THE WALL STREET JOURNAL.

Once the stuff of science fiction, facial-scanning cameras are becoming a part of daily life in China, where they're used for marketing, surveillance and social control. Video: Paolo Bosonin. Photo: Qilai Shen/Bloomberg

WORLD | ASIA | CHINA

China's All-Seeing Surveillance State Is Reading Its Citizens' Faces

In vast social-engineering experiment, facial-recognition systems crunch data from ubiquitous cameras to monitor citizens

Online Behavioral Tracking

An increasing part of our daily activities are recorded

- What we are interested in (Searches, Likes, …)
- What we read (News, magazines, blogs, …)
- What we buy (Amazon, Freshdirect, …)
- What we watch (Netflix, Hulu, …)
- What we eat (Seamless, GrubHub, …)
- Where we eat (Opentable, Foursquare, …)
- Where we go (online travel/hotel/event booking)
- What we own/owe (e-banking, credit services, Mint, …)

Mobile apps make behavioral tracking easier and more accurate

Behavioral profiles have desirable and not so desirable uses

- Recommendations, content personalization, insights, …
- Targeted advertising, price discrimination (e.g., insurance premiums based on past behavior, higher prices for high-end device users), …

Health and Activity

Health records

- How securely are they handled and stored?

Devices track our activities and health

- Activity tracking devices
- Health monitoring devices
- Mobile phones

Many upload all data to the “cloud”…

- Who can access them?

Doctor/hospital health portals managed by third parties