Who Stole My Privacy?

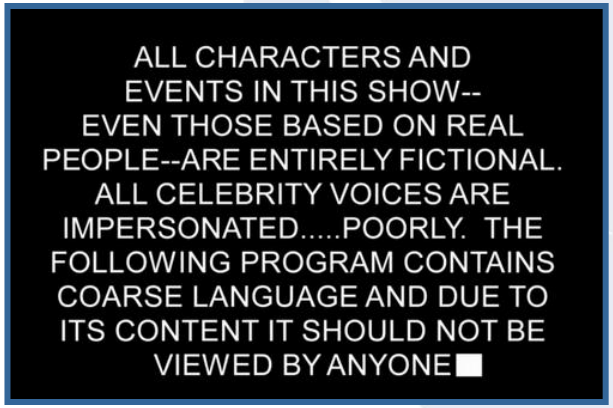
April 2013

Information Security and Privacy Office

City of Phoenix

Disclaimer

- The City of Phoenix does not endorse or disparage any commercial products, services, entities, or political candidates
- Any mentioned in this presentation are as examples only
- Most scenarios are true
  - Some were invented to fit known facts
  - All names were changed



Agenda

- Privacy definition and why you should care
- Basic safeguards
- Scenarios

What Is Privacy?

- The rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personally identifiable information
  - American Association of Certified Public Accountants
- The state of being free from unsanctioned intrusion
  - Dictionary.com (and others)
- The right to be “left alone”
  - ISPO (and others)

Why Should You Care about Privacy?

- Dignity
  - Privacy is a basic human need
- Financial impact
  - I have to pay more for goods and services based on my profile
- Personal safety
  - Do strangers know where I am?
- Ick factor
  - Monitored? Is this George Orwell's 1984?
- Stifling individualism, expression, and creativity
  - Will I still express myself knowing that I'm being monitored?

Controlling Your Privacy

- When it comes to privacy, there are
  - Things you can control
  - Things you can't control

Things You Can't Control

Parents, Experts Blast New State Database of Private Student Info

Thursday, Mar 14, 2013 | Updated 12:02 PM EDT

Parents and privacy experts are blasting a new national database that compiles personal student information for educational companies that contract with public schools.

EXCLUSIVE - U.S. to let spy agencies scour Americans' finances

By Emily Flitter and Stella Dawson and Mark Hosenball

NEW YORK/WASHINGTON | Wed Mar 13, 2013 2:31pm EDT

(Reuters) - The Obama administration is drawing up plans to give all U.S. spy agencies full access to a massive database that contains financial data on American citizens and others who bank in the country, according to a Treasury Department document seen by Reuters.

Vudu Customer Data Stolen in Office Burglary

Ben Weitzenkorn, TechNewsDaily Contributor

Date: 10 April 2013 Time: 05:41 PM ET

Things You Can Control: Basic Privacy Safeguards

- Be aware
  - Ask how your info will be used or whether it's shared
  - Example: Store asking for your zip code when you make a purchase
- Read the fine print and Website privacy policies
  - Don't blindly give out your personal information
- Support those who respect privacy
  - Give your business to responsible retailers
  - Support organizations and initiatives that build privacy into systems

Things You Can Control: Basic Digital Privacy Safeguards

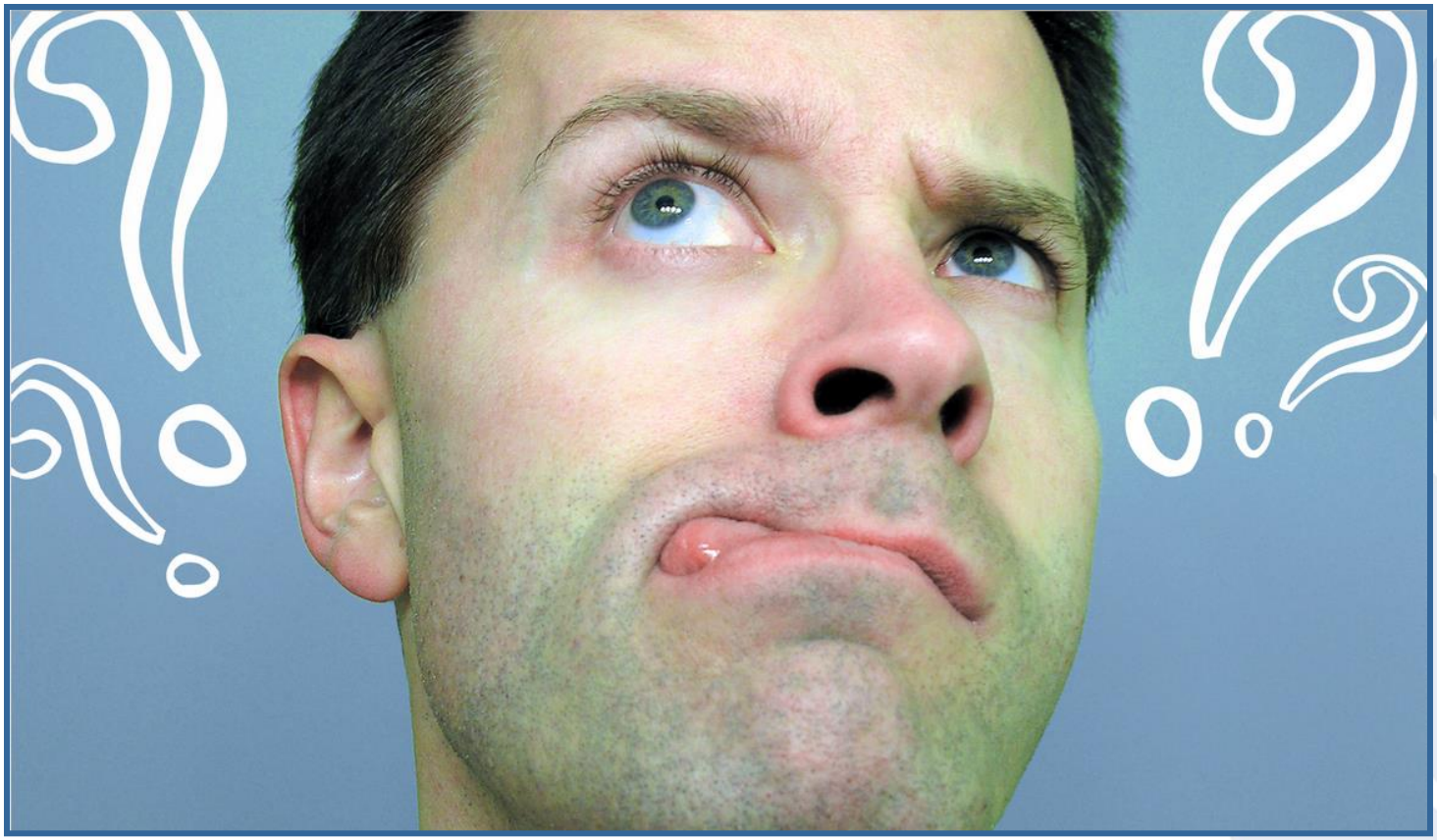
- Don’t post too much information online
  - About yourself / family, where you are, where you’ll be
  - This includes pictures and videos
- Don’t “check in” to location services, like Foursquare
- Use a strong password on your accounts
  - Use different passwords for different accounts (Facebook, banking, email, work)
  - The length of a password is more important than it’s complexity (based on new password-cracking techniques)

- See phoenix.gov/infosec Resources page for more

Maya Got a Bill for an Appendectomy

- But she never had one
- Maya called Texas hospital to protest the bill
  - Maya lives in Phoenix
- She had to fly there and lift her shirt to prove she didn't have an appendectomy
  - Maya doesn't have a scar

What Happened to Maya?



Medical ID Theft Rises (Again)

- About 2 million Americans fall victim to medical ID theft every year
  - The cost per victim rose from $20,663 in 2011 to $22,346 in 2012
  - The total cost jumped from $30.9 billion last year to $41 billion
- 45% of medical ID theft victims end up paying their health-care provider or insurer for charges incurred by the thieves
  - Victims don't typically have any other recourse
- 50% of victims say they know the person who victimized them
  - 31% say they allow family members to use their IDs to get medical services (aka familial fraud)

- Source: Ponemon Institute's Third Annual National Study on Medical Identity Theft

Signs of Medical ID Theft

- Explanation of Benefits (EOB) statement, Medicare Summary Notice, or bill for medical services you didn't receive
  - Check the name of the provider, the date of service, and the service provided
- Call from a debt collector about a medical debt you don't owe
- Medical collection notices on your credit report that you don't recognize
- Notice from your health plan saying you reached your benefit limit
- Denial of insurance because your medical records show a condition you don't have
- Numerous errors in your medical records

How to Resolve Medical ID Theft

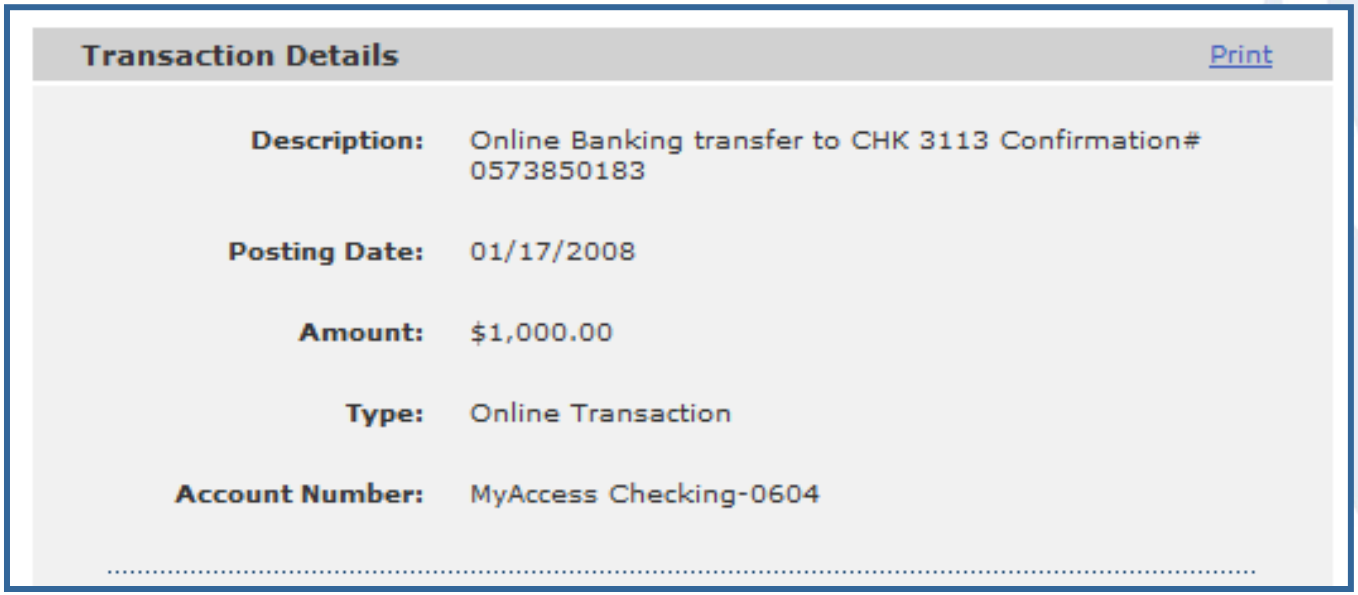
- Get copies of your medical records and check them for errors
  - Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and location where a thief may have used your information
  - Example, if a thief got a prescription in your name, ask for records from the health care provider who wrote the prescription and the pharmacy that filled it
- Ask each of your health plans and medical providers for a copy of the “accounting of disclosures” for your medical records – a record of who got copies of your records from the provider
  - The accounting shows who has copies of your mistaken records and whom you need to contact
- More info at: http://www.consumer.ftc.gov/articles/0171-medical-identity-theft

Who Stole Maya's Medical Identity?

- An illegal immigrant got ahold of Maya's social security number and stole her identity
- Warning: Medical ID theft can be life threatening if wrong information ends up in your medical file
  - Blood type, allergies, conditions…

Fraudulent Money Transfer

- Sylvia and James were getting a divorce, so they separated their bank accounts
- A few months later, Sylvia discovered a fraudulent transaction in her bank account
  - Transfer of $1,000 from Sylvia's checking account (0604) to another checking account (3113)

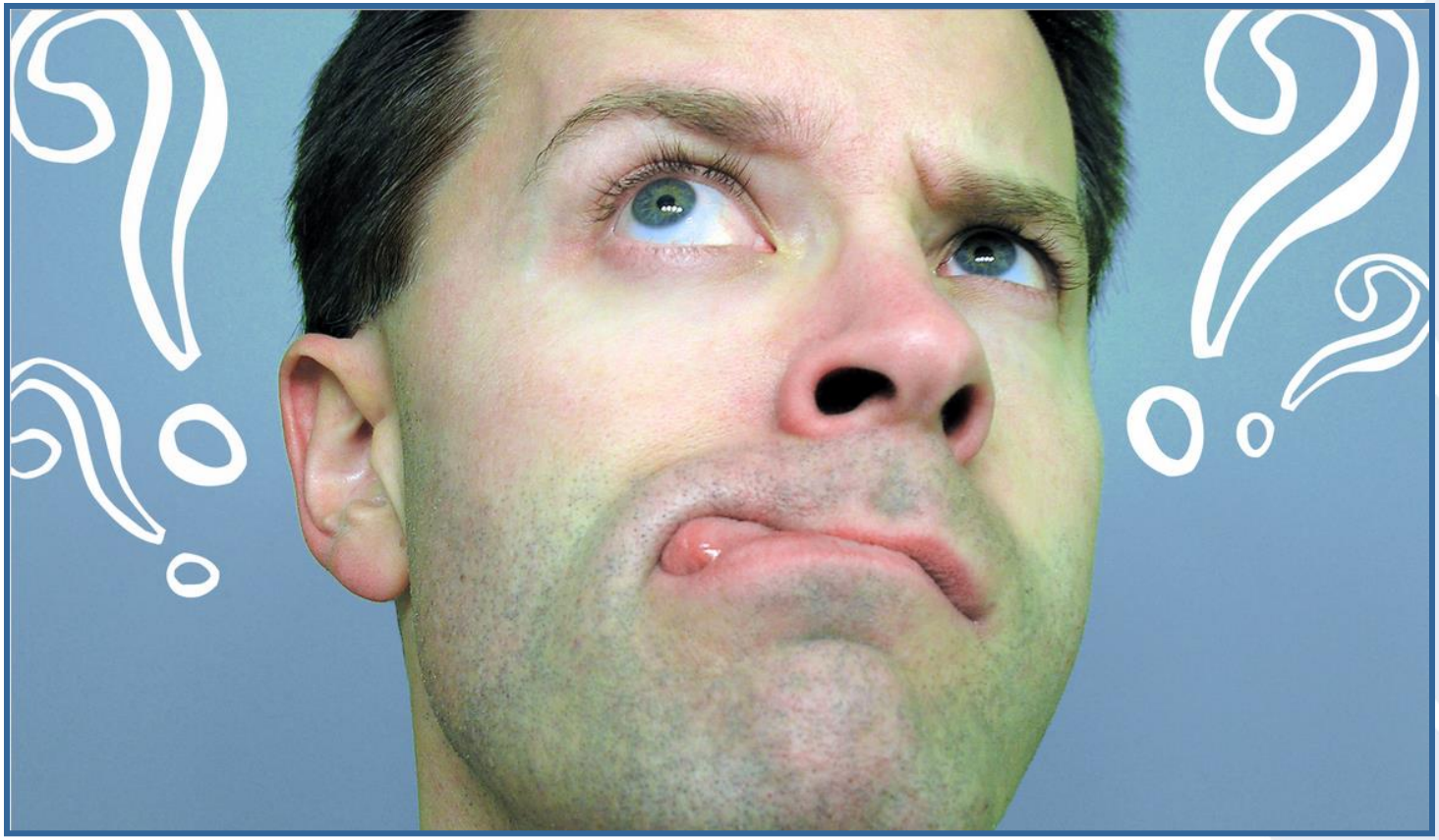


Transaction Details Print

Description:	Online Banking transfer to CHK 3113 Confirmation# 0573850183
Posting Date:	01/17/2008
Amount:	$1,000.00
Type:	Online Transaction
Account Number:	MyAccess Checking-0604

Who Stole Sylvia's Money?

- Remember – James was taken off Sylvia's account



Resolving the Fraudulent Activity

- Sylvia reported the incident to the bank with documentation showing she was the sole account owner
  - Bank confirmed Sylvia was the sole account owner
- Sylvia called the police
  - Just to have a police report on record
- Bank's fraud department researched the issue
- Bank determined that James had used his online account access to transfer the money to his account
  - At the time (2008), removing a person from the account did not remove their online access to the account
- Bank transferred money from James' account back into Sylvia's
- Police recommended not filing charges against James
  - Considered it a "domestic dispute"

Revenge Porn and Other Hazards

- When a relationship ends badly, every racy photo, text, password, and account you shared with your ex becomes a potential security problem
  - A vengeful ex-lover could leak pictures online, use your passwords to cyberstalk you, or exact other forms of digital revenge
- One in 10 exes has threatened to post a revealing photo of a former partner online, and 60% of those people followed through with it
  - McAfee “romance-themed” survey, February 2013

It’s Not Just Your Ex

- More than 50% of people share their passwords with a partner
  - “Sharing passwords is seen as a sign of love and devotion, a sign of commitment”
- More than 56% of people snooped on their partner’s social media pages and bank accounts
  - 48.8% looked at their e-mails
- During their marriage, James tracked Sylvia’s movements by her debit card spending
  - Gas station, restaurant, grocery store…

Protect Yourself

- Resist the urge to send intimate content
  - Texts, emails, pictures, video
- Once it's shared, you've lost all control over it
- Digital content lives forever

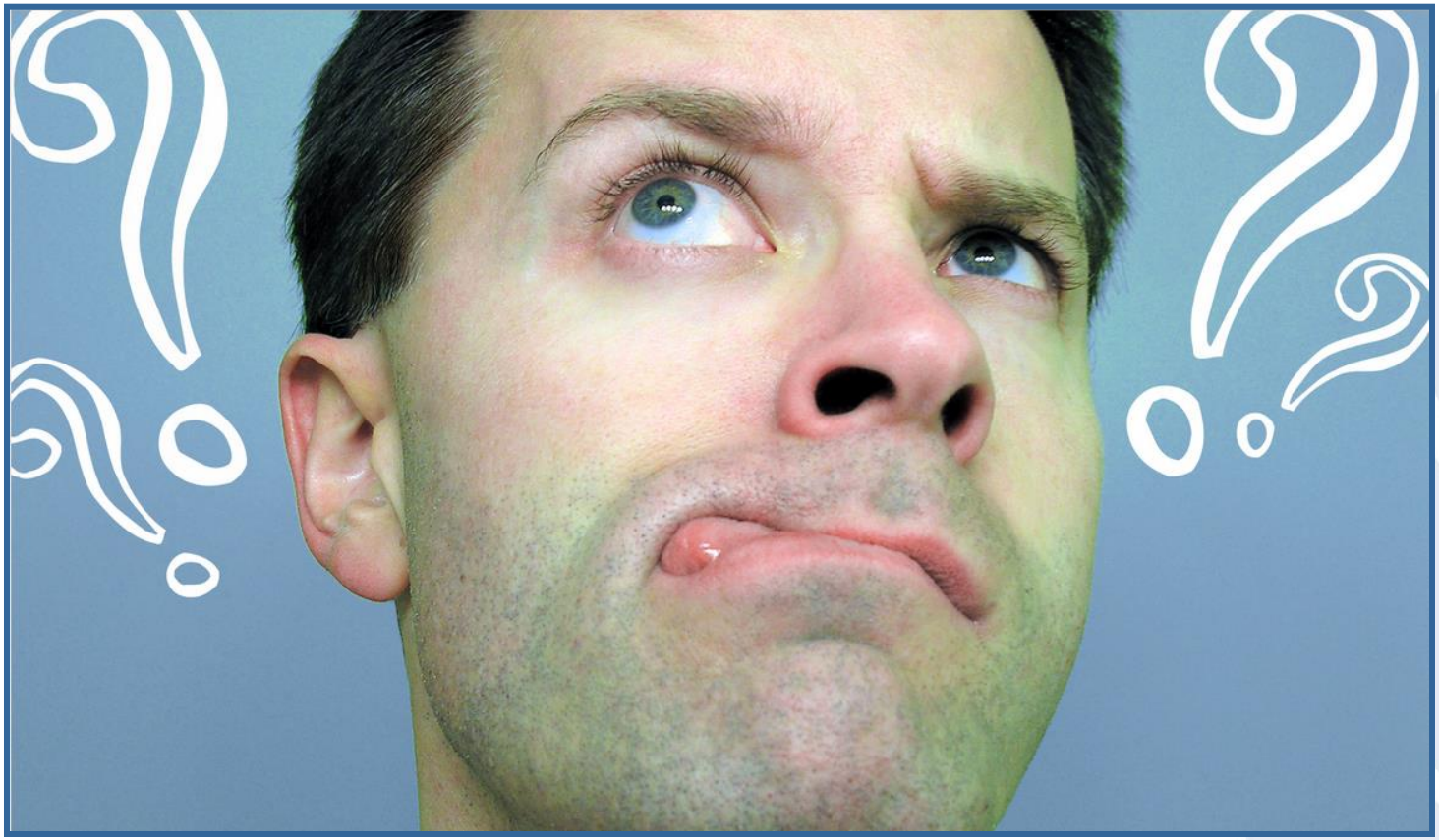
- Change all your passwords ASAP
  - Change them before the break-up and "forget" to tell your soon-to-be ex
- Put a password / PIN on your digital devices to prevent snooping

- Consider trying to reason with your ex

Angry Father

- Pete walked into a Target outside Minneapolis and demanded to see the manager
  - He was clutching coupons that had been sent to his daughter, and he was angry
- “My daughter got this in the mail! She’s still in high school, and you’re sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?”
  - The manager apologized and then called a few days later to apologize again
- On the phone, though, the father was somewhat abashed
  - “I had a talk with my daughter. It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August. I owe you an apology.”

How Did Target Know that the Teen Was Pregnant (Before Her Dad)?



Marketing 101 According to Target

- Once consumers' shopping habits are ingrained, it's incredibly difficult to change them
  - When parents have a newborn, are exhausted and overwhelmed, their shopping patterns and brand loyalties are up for grabs
    - That's why new parents are barraged with offers and ads
- So Target wants to reach pregnant women early
  - Target marketers want to send specially designed ads to women in their second trimester
    - That's when most expectant mothers begin buying all sorts of new things, like prenatal vitamins and maternity clothing
- "We knew that if we could identify them in their second trimester, there's a good chance we could capture them for years. As soon as we get them buying diapers from us, they're going to start buying everything else too."

Target Analyzes You (Like Other Companies Do)

- Whenever possible, Target assigns each shopper a unique Guest ID number that keeps tabs on everything they buy
  - "If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you or visit our Web site, we'll record it and link it to your Guest ID."
- They perform extensive data analysis on you and your purchases
  - "Just wait. We'll be sending you coupons for things you want before you even know you want them."

Behavioral Advertising

- Online behavioral advertising – the practice of tracking your online activities in order to deliver advertising tailored to your interests

- And not just tracking your interest, but also predicting your interests
  - Age, sex, location
  - Hobbies, estimated income, medical conditions
  - Websites, books, tv, movies viewed/bought
  - Opinions posted, travel taken, key words searched

What Target Knows About You

Info Target Collects

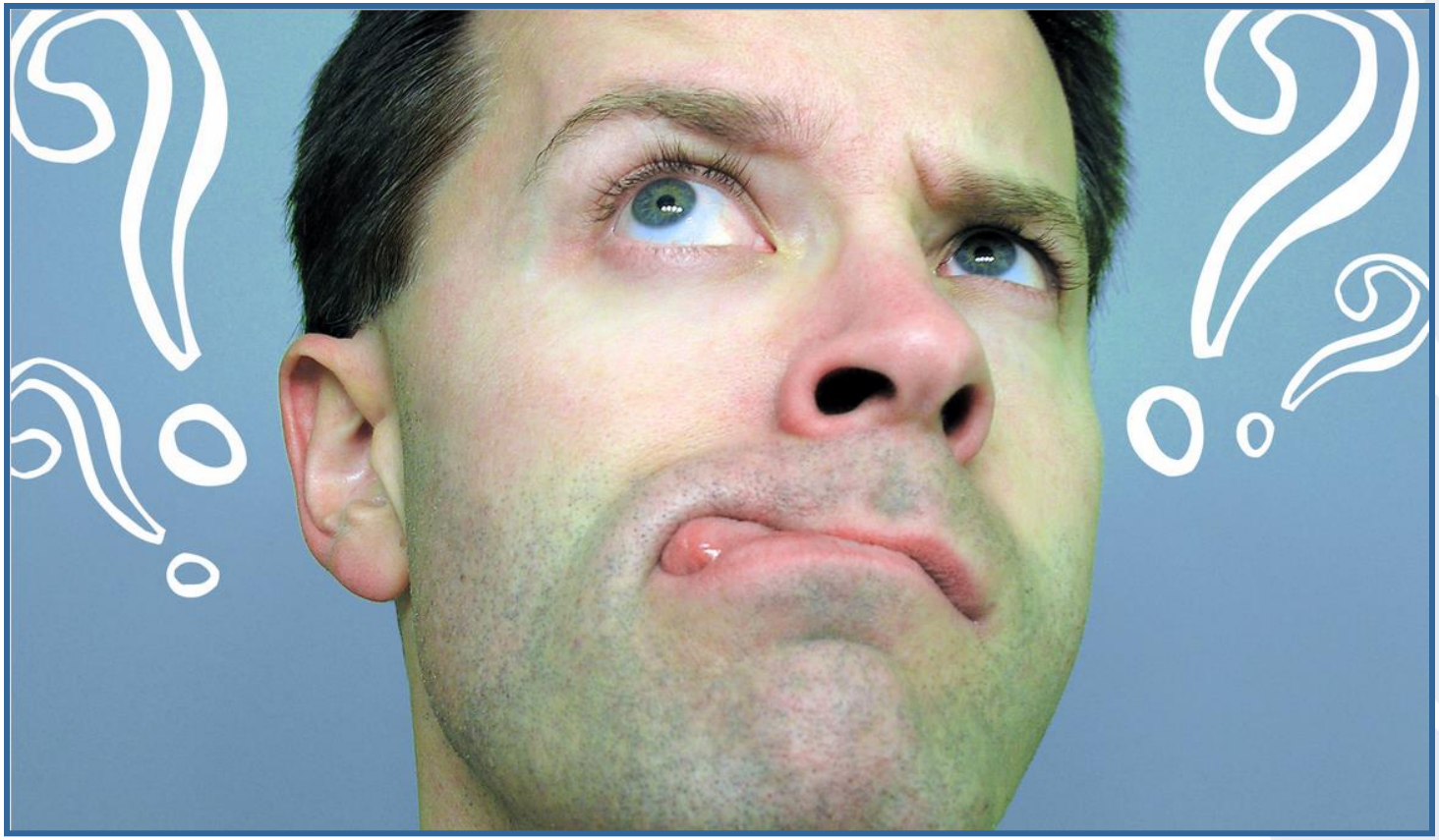
- Marital status
- Children
- Where you live
- Time to drive to the store
- Estimated salary
- Whether you've moved recently
- What credit cards you carry
- What web sites you visit

Info Target Purchases

- Ethnicity
- Job history
- Magazines and other reading habits
- Whether you've ever declared bankruptcy or gotten divorced
- Year you bought (or lost) your house
- College alma mater
- Topics you talk about online
- Preferred brands of coffee, paper towels, cereal, or applesauce
- Political leanings
- Charitable giving
- Number of cars you own

True or False

- Amazon knows more about me than my mother



Tracking Software

- Top 50 U.S. websites installed an average 64 pieces of tracking technology onto the computers of visitors, usually with no warning
- A dozen sites each installed more than 100
- The nonprofit Wikipedia installed none
  - Source: Wall Street Journal study published August 2, 2010

The Trackers

- Cookies, Flash cookies, and beacons
  - Put on your computer when you visit a website
- Simple cookies record websites you visit and maybe your personalizations (colors, password…)
- New tools scan in real time what you are doing on a Web page, then instantly assess your location, income, shopping interests, and even medical conditions

Third Party Tracking Files – Complex Trackers

- The first time you visit a site, it installs a tracking file, which assigns your computer a unique ID number
- Whenever you visit another site affiliated with the same tracking company, it notes where you were before and where you are now
- Over time, the company builds a robust profile about you

Cookie Consent

- Per the European Privacy Directive, websites must ask visitors for their consent before they can install most cookies
  - Officially, it's Article 5(3) of the EU Directive 2009/136/EC, known as the "Cookie Law" of the E-Privacy Directive
- So if you'll see a notification when you visit a European website
- The U.S. does not have any law like this

Tracked Info Is “Anonymous”

- Trackers *do not* collect your name

Pop Quiz

- How many pieces of anonymous information are needed to identify you?
  - Example: zip code, age, gender, car model, dog owner, type of computer browser used…

Pop Quiz

- How many pieces of anonymous information are needed to identify you?
- In the field of re-identification science, it's "33 bits of entropy"
  - Information-science researchers refer to random pieces of information as "entropy"

Data Brokers

- Data brokers collect details about consumers and sells them
  - Example: Acxiom collects info on more than 700m consumers across the globe and sells them to more than 7,000 clients
    - They track everything from a person's estimated income to his political leanings, shopping patterns, and exercise habits

- "Consumers are often unaware of the existence of data brokers as well as the purposes for which they collect and use consumers' data"
  - Federal Trade Commission, December 2012

- No current laws in the US require that data brokers maintain the privacy of individual's data unless they are used for credit, employment, insurance, housing or other similar purposes

Acxiom: Here's what we know about you

- For its marketing information business, consumers now can visit Acxiom's website to opt out of targeted ads based on Acxiom data
  - But we have no way to access the data collected

This is GREAT!

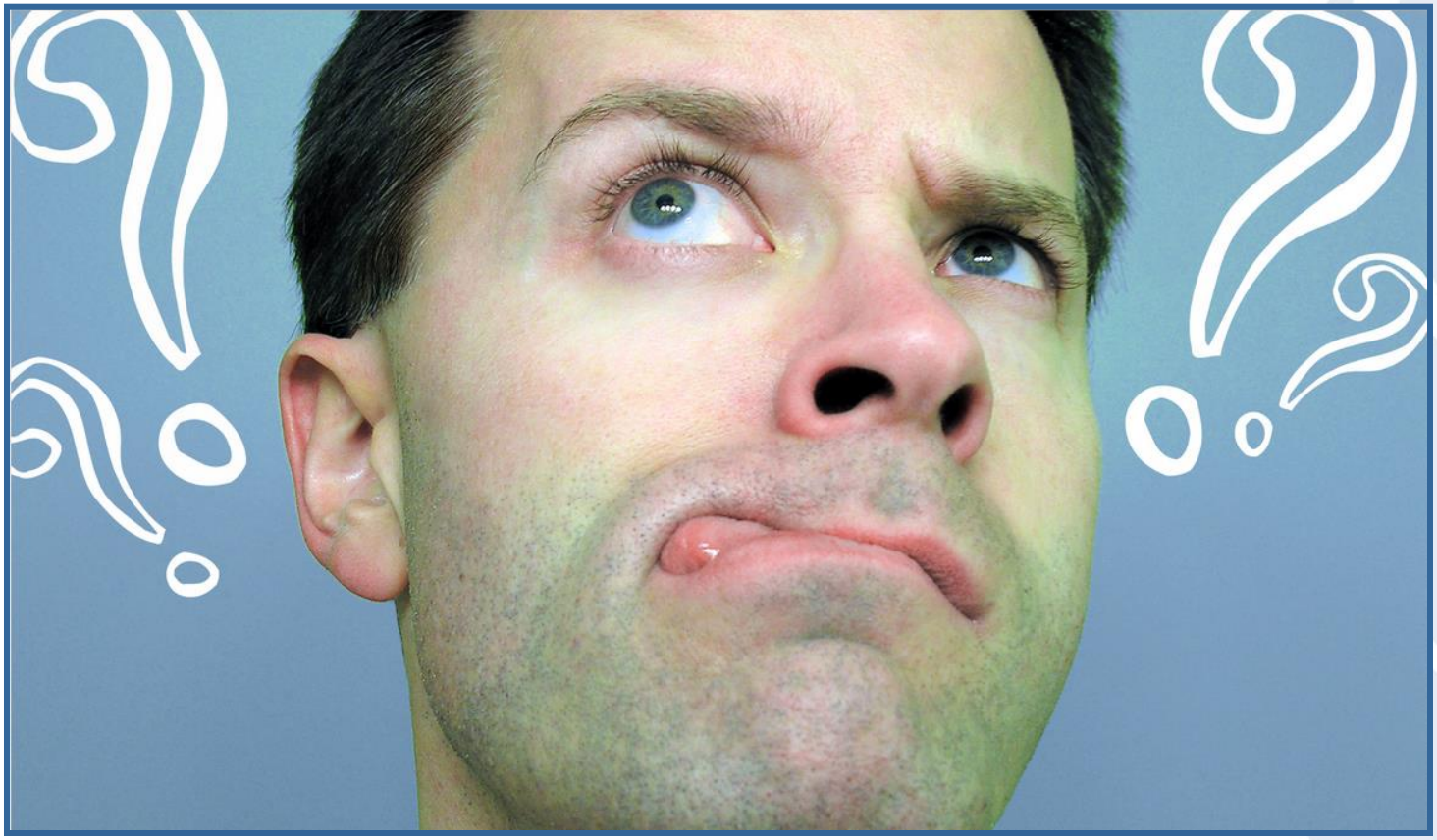
- They're readying a service that will reveal to people what it knows about them
  - Should be available sometime this year, but some technical and logistical hurdles remain
  - Company is attempting to secure the service so that individuals will not fall victim to identity theft from others accessing their data

Just an FYI… Internet Advertising

- Internet advertising revenues in the United States totaled $17.0 billion for the first six months of 2012
  - Revenues for the first six months of 2012 increased 14% over the first six months of 2011
  - Based on an industry survey conducted by PwC and sponsored by the Interactive Advertising Bureau

Why Would We Want Tracking and Behavioral Advertising?

- What benefit do we get from tracking and/or behavioral advertising?



Benefits of Surveillance

- Public safety
  - Surveillance (cameras) can prevent and detect crime

Terrorists: Tamerlan Tsarnaev (right) was killed during an exchange of gunfire with police on Wednesday night. His younger brother Dzhokhar (left) is still on the run and reportedly has explosives strapped to his body

  - Suspects in the Boston Marathon bombings, as of 4/19/2013

Benefits of Behavioral Advertising

- You get relevant offers for products and services
- Your price may be different, because the vendor knows your demographics
  - Warning: Price might be higher
- Services offered to you might be different, because the vendor knows your demographics
- It takes effort to stop / avoid behavioral advertising and tracking / surveillance

Who Pays More for Insurance?

Jim

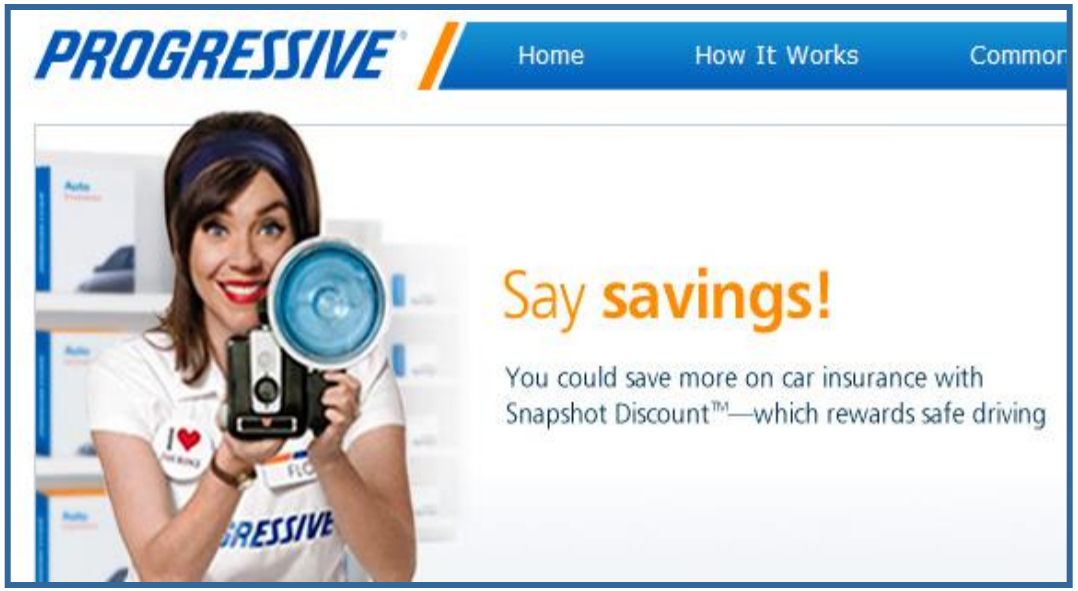
- Buys fruits and veggies
  - Grocery loyalty card
- Has a gym membership
  - Gym's "business partners"
- Owns a home
  - Insurance records, public records
- Shops at Macy's
  - Store credit card
- Reads "Smithsonian" magazine
  - Subscription records

John

- Buys frozen pizza, chips, and snack cakes
  - Grocery loyalty card
- Smokes
  - Entered in "Marlboro Ranch" contest
- Single or "looking"
  - Match.com's "business partners"
- Reads "Guns and Ammo" magazine
  - Subscription records

Surrendering Privacy Example: Progressive Insurance Snapshot

- A usage-based insurance rating program
  - Customers opt-in and get a device that plugs into the data port on vehicles that are 1996 or newer
- Snapshot device records driver behavior
  - Vehicle speed and time information, Vehicle Identification Number, G force (in some devices), as well as when the device is connected and disconnected from the vehicle

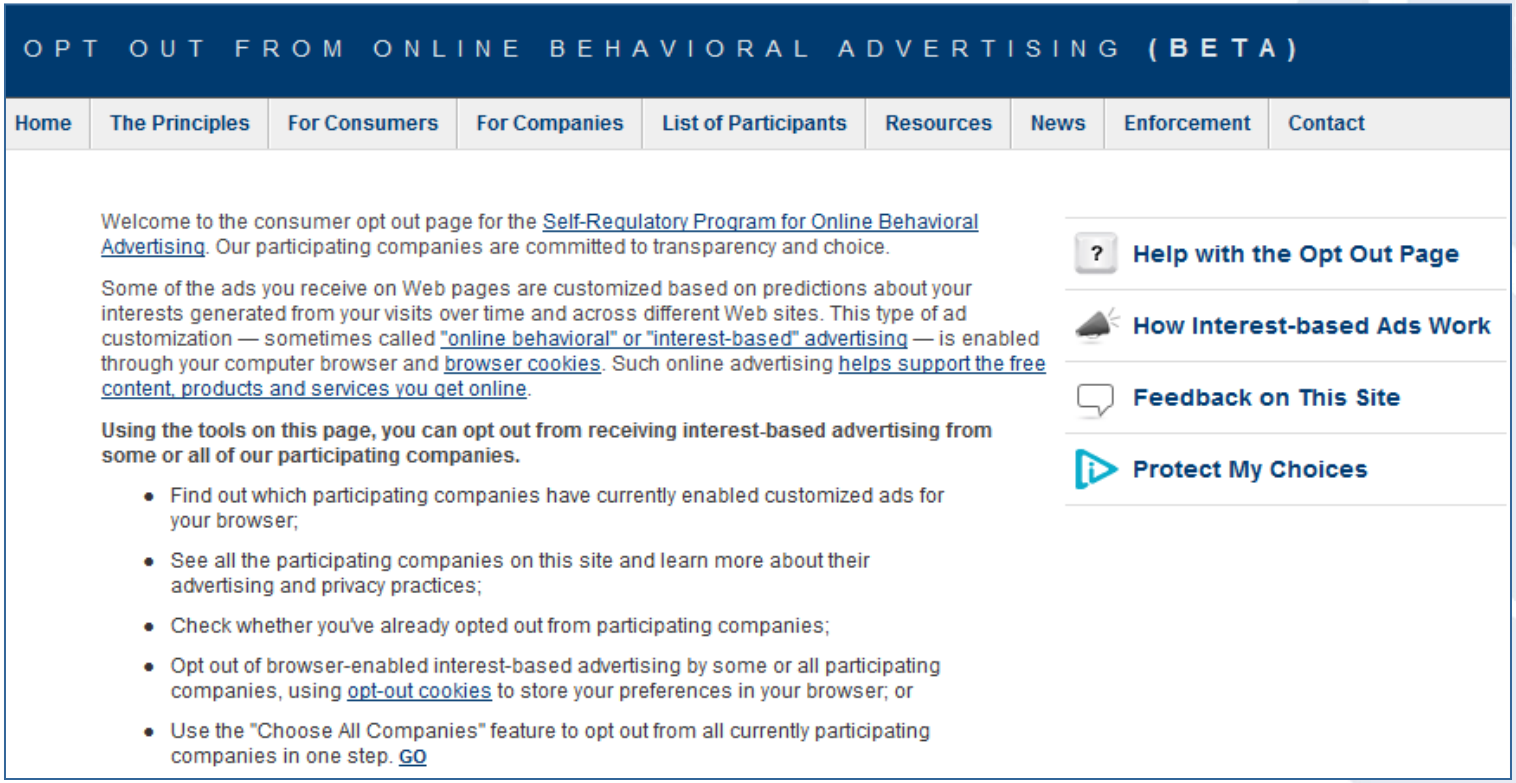


Example: AccuquoteLife.com

- July 2010, life-insurance site tested a system showing visitors life insurance policies based on visitors' "determined" demographics
  - Suburban, college-educated baby-boomers saw a default policy of $2 – 3 million
  - A rural, working-class senior citizen saw a default policy for $250,000

Protect Your Privacy – Opt Out

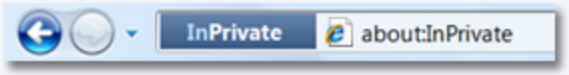
- Legitimate organizations provide opt-out instructions in their privacy policies
  - Example from Digital Advertising Alliance's (DAA) Self-Regulatory Program for Online Behavioral Advertising:



Use Browser Privacy Controls

InPrivate is turned on

When InPrivate Browsing is turned on, you will see this indicator



InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.

To turn off InPrivate Browsing, close this browser window.

Firefox Windows 7/Vista Firefox 20

EDITING TOOLS

RELATED ARTICLES

Settings for privacy, browsing history and do-not-track

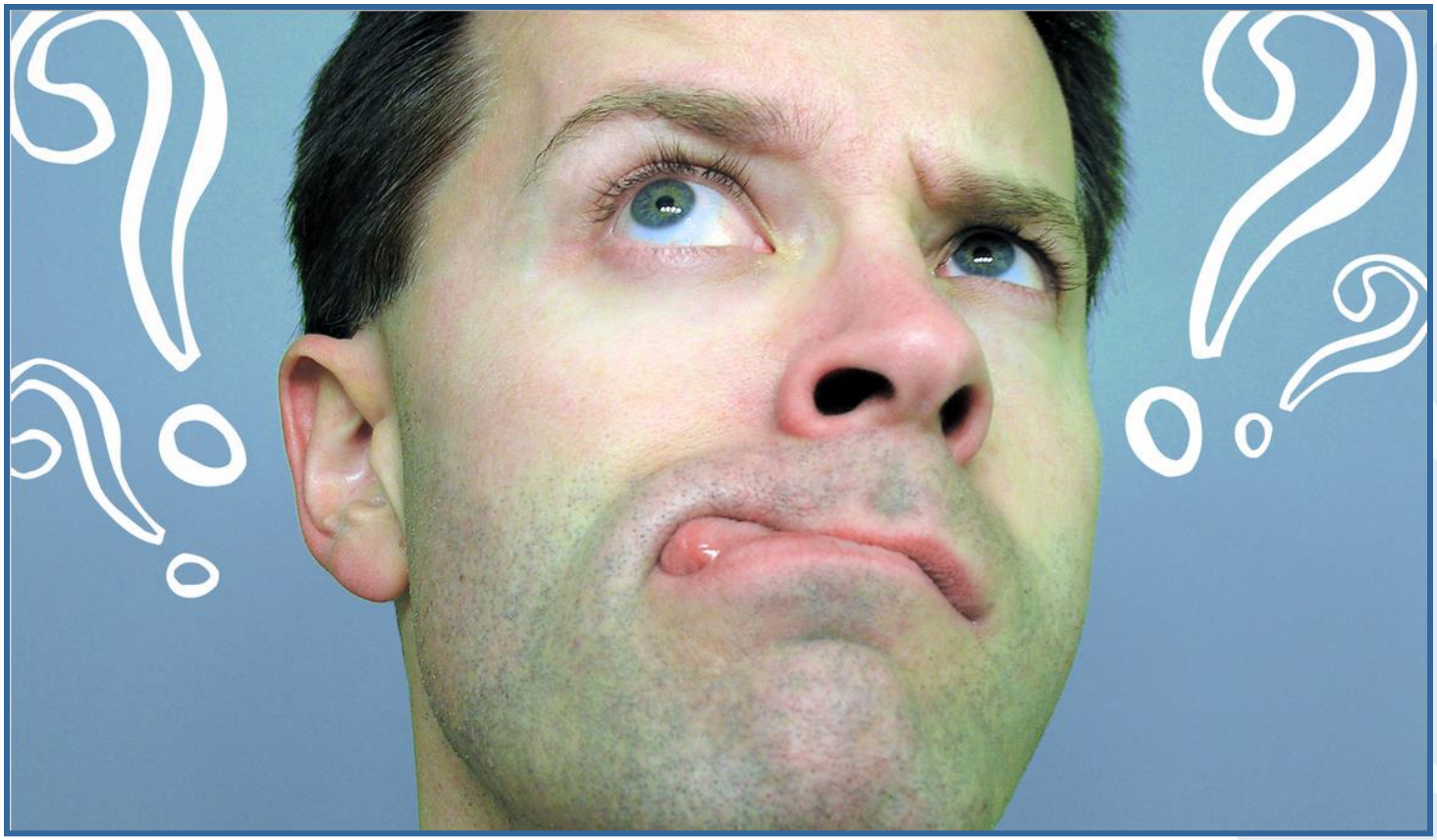
March 18, 2013, 1:20PM

How To: Chrome Browser Privacy Settings

The Bigamist

- Jim, a Corrections Officer in Tacoma, WA married a woman in 2001 and moved out in 2009
- Then he changed his name in December and remarried without divorcing his first wife
- Wife #1 alerted authorities and Jim was arrested on bigamy charges

How Did Wife #1 Know Hubby Remarried?

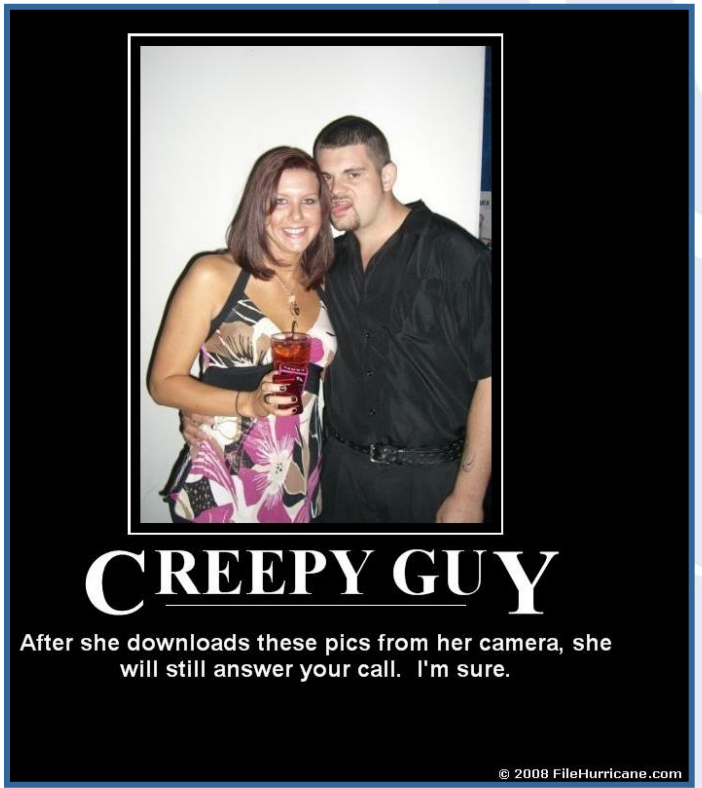


Facebook's People You May Know

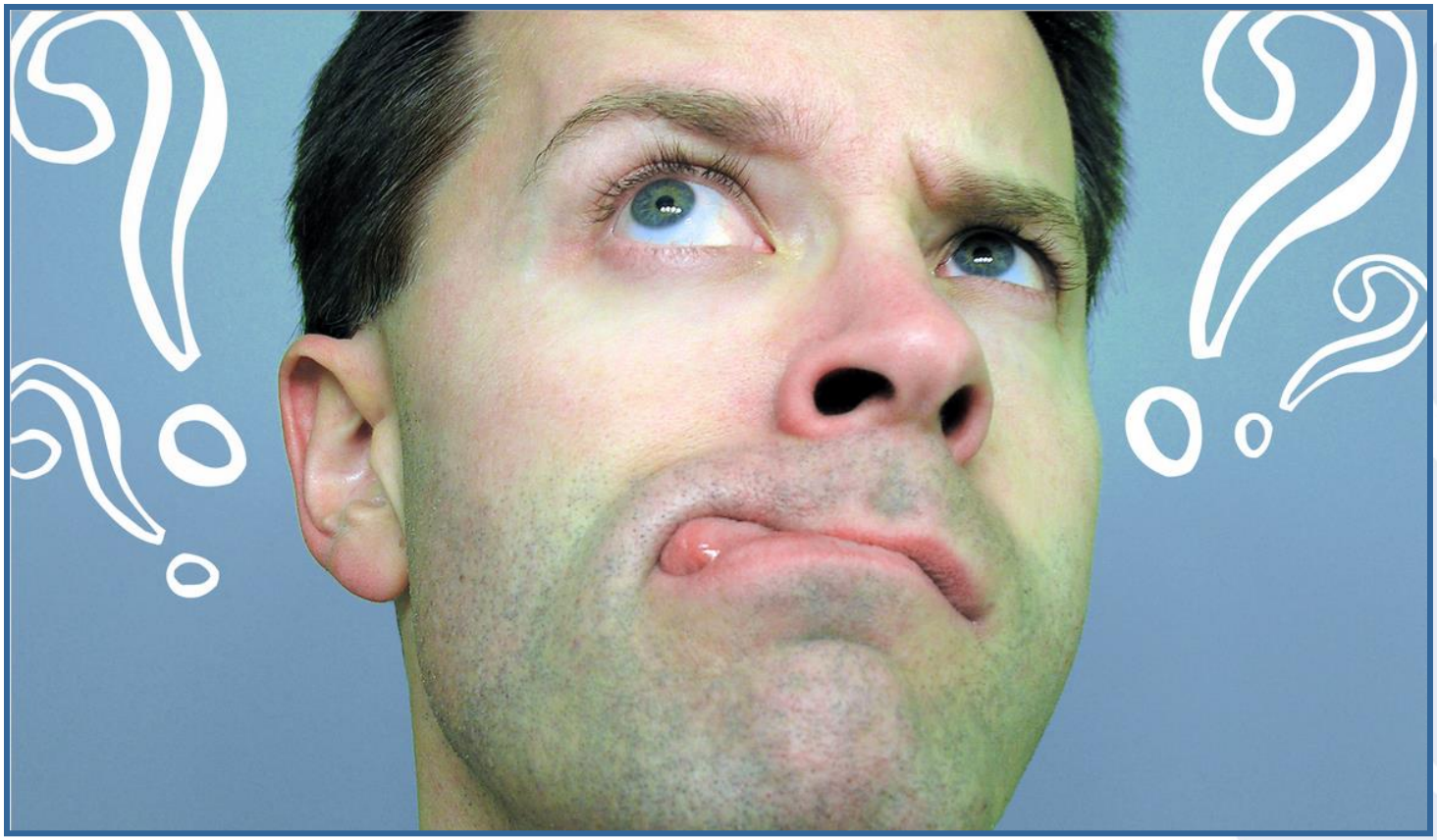
- Facebook's automated friend-connection software detected the connection of both wives to the same man
- Facebook suggested that wife #1 friend wife #2
  - "Wife #1 went to wife #2's page and saw a picture of her and her husband with a wedding cake"
    - Pierce County Prosecutor Mark Lindquist
- People You May Know is an automated Facebook feature that shows you people on Facebook that you likely know
  - Based on mutual friends, work and education information, networks you're part of, imported contacts and many other factors
  - Facebook does not send friend requests to anyone that shows up in this list on your behalf

Toni Out-on-the-Town

- Toni loved going out with her friends
  - She went to bars, dance clubs, coffee houses…
- Everywhere she went, she kept seeing the same guy
- He was creepy
- Toni was scared



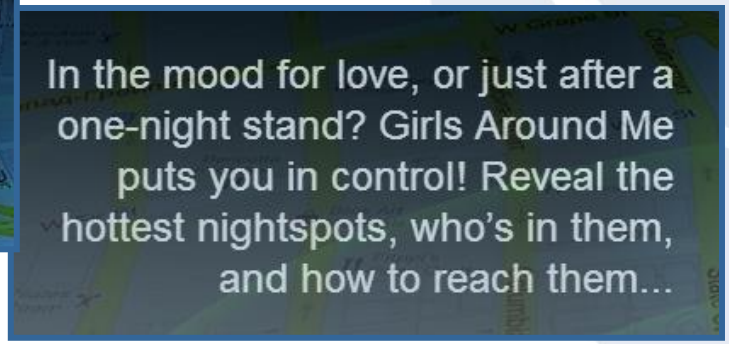
How Did Creepy Guy Know Where to Find Toni?



Girls Around Me App

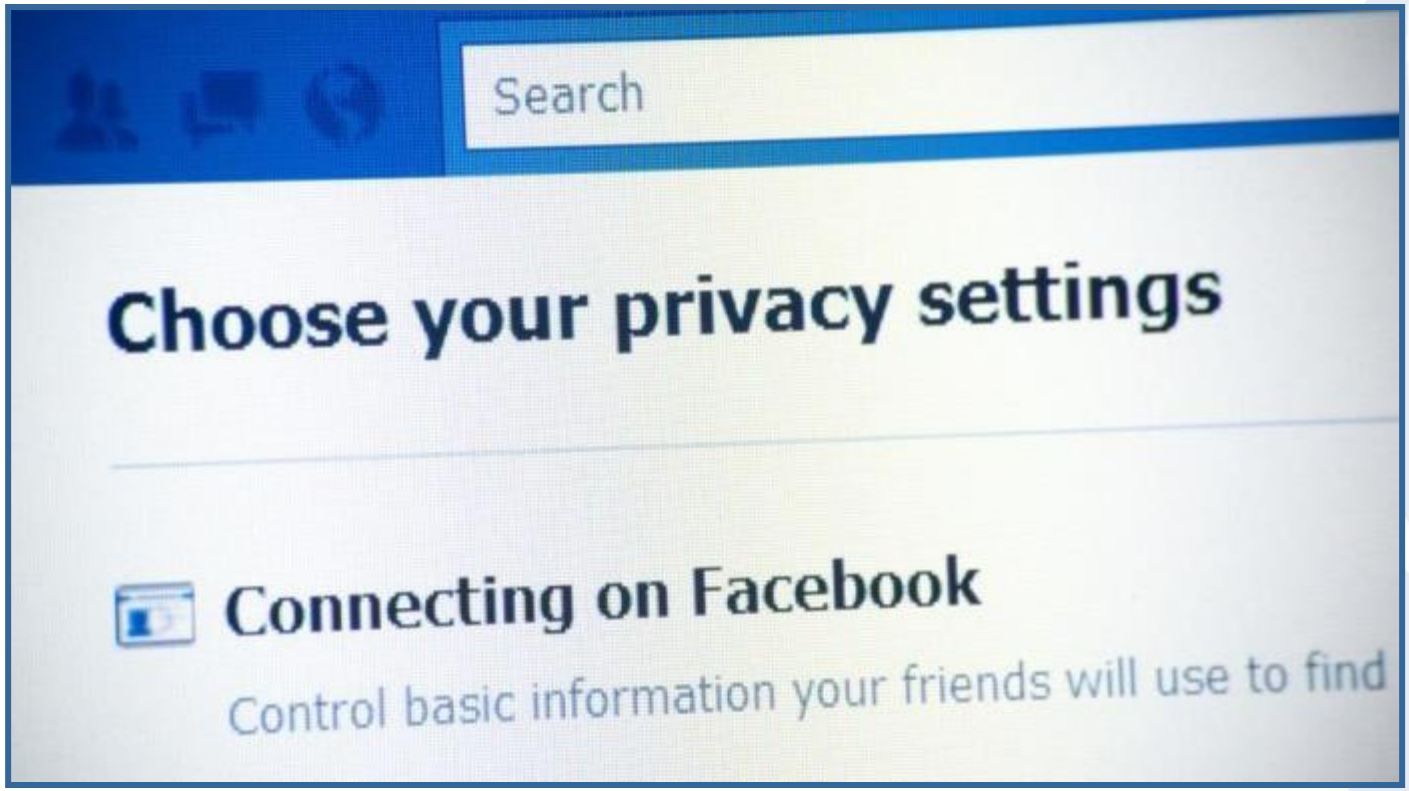
- "… scans your surroundings and helps you find out where girls or guys are hanging out
  - Browse photos of lovely local ladies and tap their thumbnail to find out more about them"

- Uses publicly available information retrieved from the Foursquare and Facebook



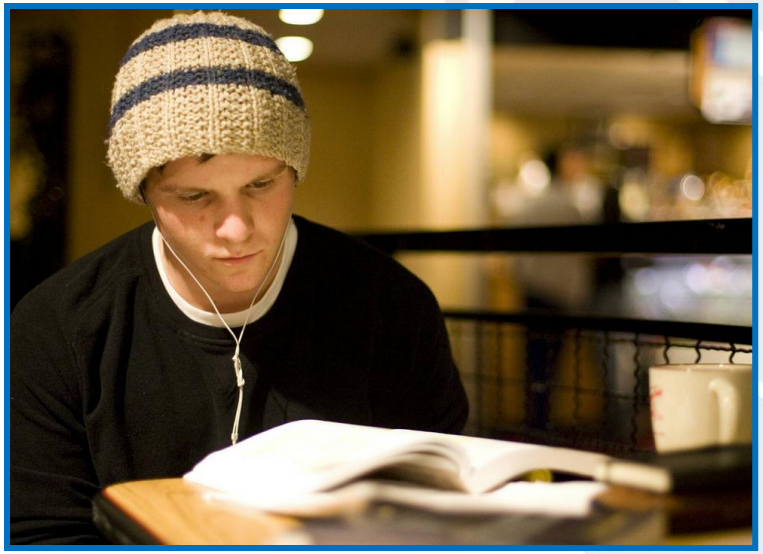
Double-Check Your Privacy Settings

- Don’t post where you’re going and where you are
- And don’t “check in” everywhere you go

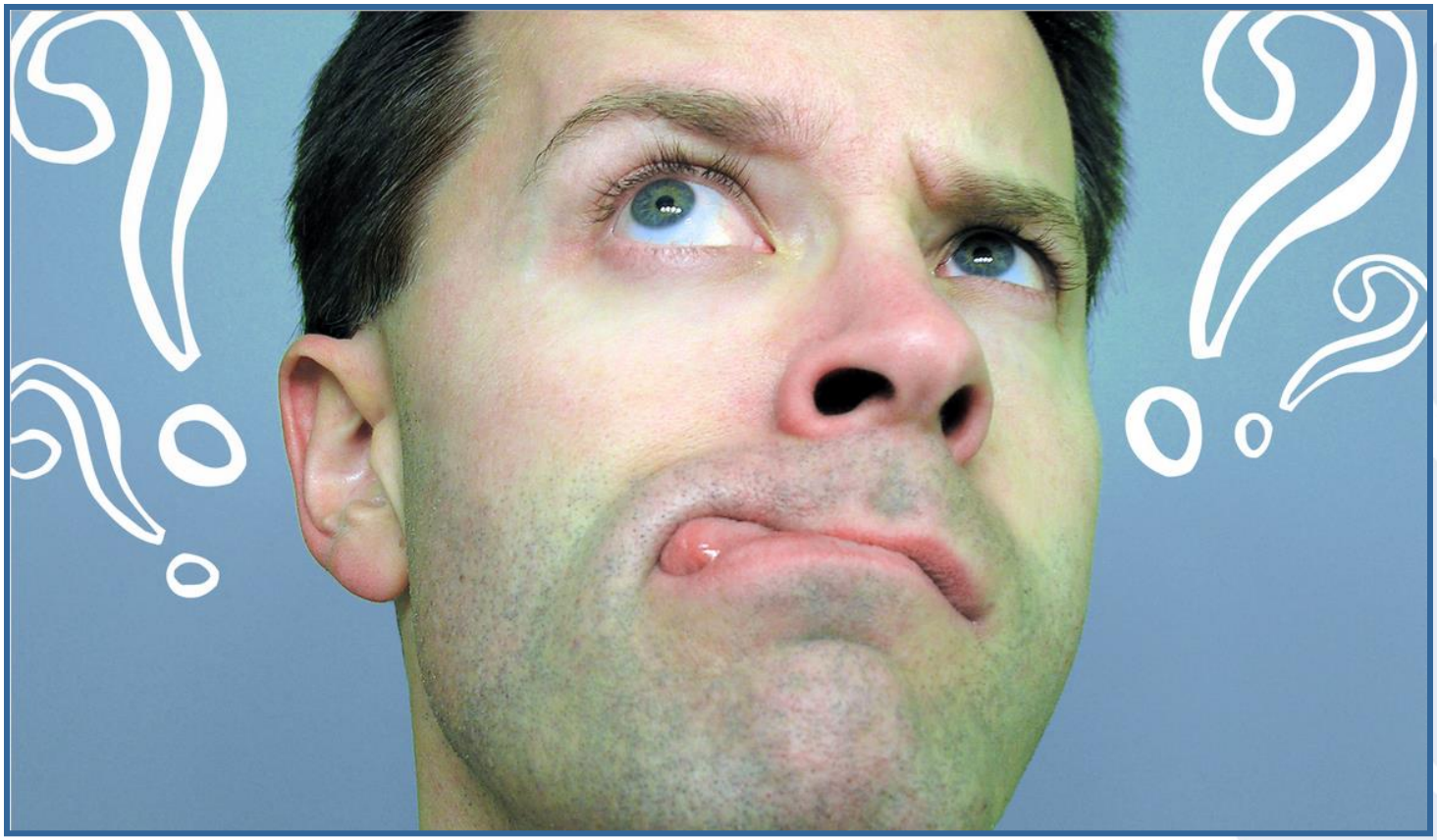


Nick Fails Class

- Nick attends Clemson University
- He fails his Management 101 final exam and begs instructor to take it again
  - Nick says he studied, but just didn't understand the material
- Instructor says no and fails Nick
  - She knows he didn't study

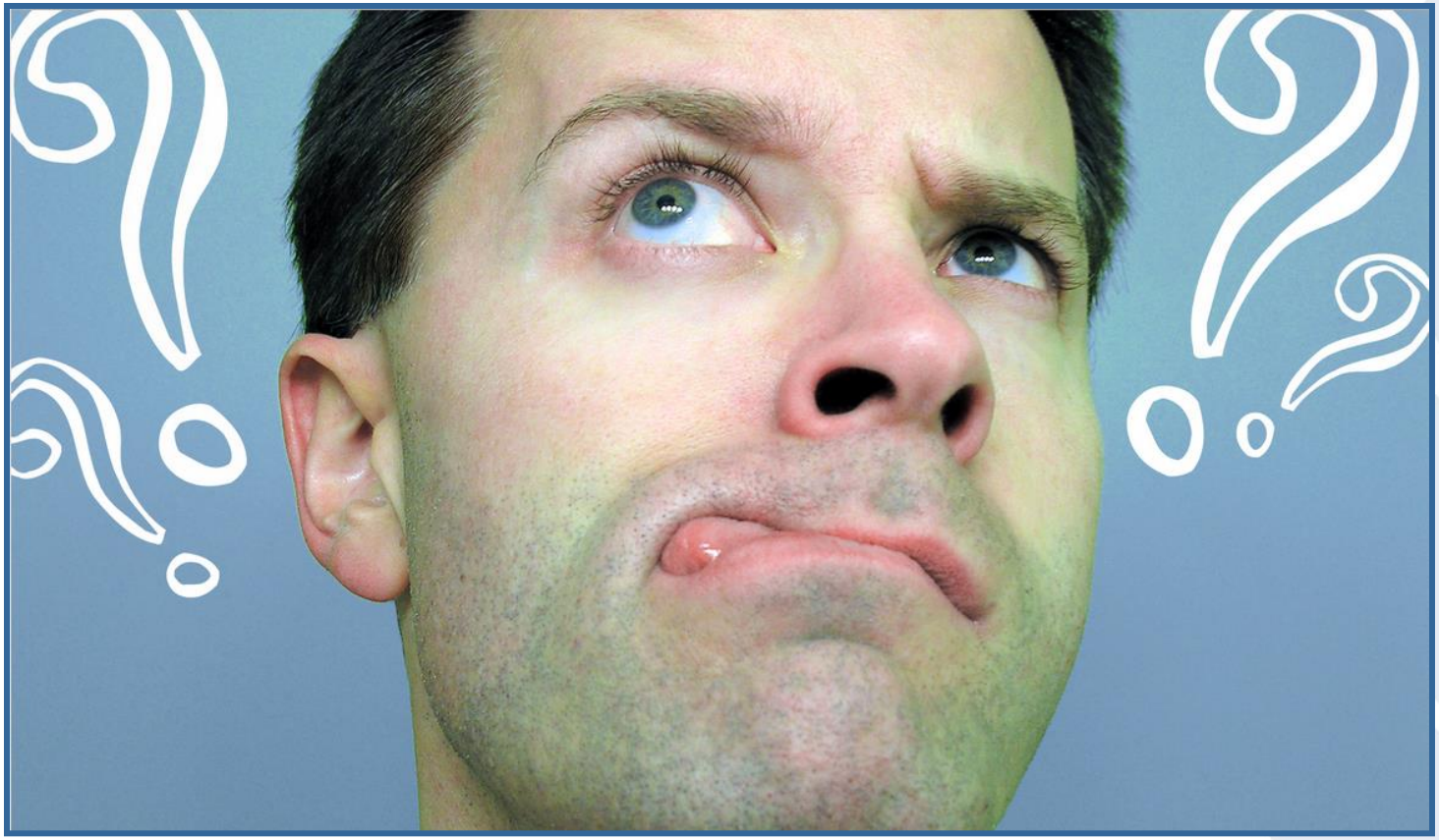


How Did the Instructor Know?



How Did the Instructor Know?

- Hint: Management 101 uses a digital textbook



How Did the Instructor Know?

- CourseSmart, a Silicon Valley start-up, allows teachers to track their students' progress with digital textbooks
  - They know when students are skipping pages, failing to highlight significant passages, not bothering to take notes, or simply not opening the book at all

- "It's Big Brother, sort of, but with a good intent"
  - Tracy Hurley, Texas A&M Dean, School of Business

eReader Privacy

Can they monitor what you're reading and how you're reading it after purchase and link that information back to you? Can they do that when the e-book is obtained elsewhere?

Google Books	Amazon Kindle	Barnes & Noble Nook	Kobo	Sony	OverDrive	IndieBound	Internet Archive	Adobe Content Server
Yes/N/A Logs specific book and page viewed on website. Stores last five pages of each book read. May also track annotations. Cannot use for e-book obtained elsewhere.	**Yes/Unclear** Stores last page read and may store annotations, highlights, markings, etc.	**Unclear** Presumably stores last page read, but Privacy Policy and Terms of Use are unclear as to other stored data.	**Unclear** Stores last page read and content deletions. May store annotations, bookmarks, highlighting etc. on servers in Canada.	**Unclear** Sony's privacy policy does not indicate whether it stores information about reading after purchase.	**Unclear** Overdrive's privacy policy does not indicate what information it stores, other than to say that the service uses cookies to store information about web usage.	**Unclear** The privacy policy does not indicate whether the reader app has the capability to store information about reading. However, since the books come through Google Books, that policy (referenced above), which does report information about reading to Google, presumably will apply.	Archive.org does not collect user-specific (including IP addresses) information when freely available content is read/downloaded. Restricted content can be borrowed through OpenLibrary.org. Borrowing requires a user account with a verified email address. The Archive knows which user has which book checked out while the loan is active, but once the book is returned we do not retain the loan information by user. OpenLibrary.org does not retain IP addresses.	**No** The Adobe Content Server software cannot monitor what a user reads.

- Read more at https://www.eff.org/pages/reader-privacy-chart-2012

AZ Reader Privacy

- March 2013: The Arizona legislature has been considering a bill that would include digital books under state law protections that would prevent disclosure of public library records. SB 1099 passed the House in a 57-1 vote earlier this month.

Do you own your e-books?

- No – you only license them
  - Unlike the owners of a physical tome, you don't have the unlimited right to lend an e-book, give it away, resell it or leave it to your heirs
  - If you bought it for your iPad, you won't be able to read it on your Kindle
  - And if Amazon or the other sellers don't like what you've done with it, they can take it back, without warning
- In the non-digital world, copyright ends with the first sale of each copyrighted object
  - Copyright is safeguarded by the limitations of physical transfer – once the book is given or loaned, the original buyer no longer has access to it
- In digital world, technology allows infinite copies to be made with no loss of quality
  - You can give away an e-book and still have it to read
  - Unrestricted transferability becomes a genuine threat to the livelihood of authors, artists, filmmakers, musicians

Protect Your Privacy

- Before buying a device or app, check its privacy policy
- Choose products and services that
  - Collect only info needed to do their job
  - Allow you to opt-out
  - Don’t share your data with unrelated third-parties
- See phoenix.gov/infosec Resources page
  - Mobile Device Security presentation
  - Safer Social Networking 2013 presentation

Learn More!

There are a lot more presentations on phoenix.gov/infosec

Look on the Resources page

Cyber Bullying	Safer Social Networking presentation
eMail Hoaxes	Scams and Fraud presentation
eMail Threats	Phishing presentation Scary Internet Stuff presentation
Encryption	Encryption 101 presentation
Hackers and Other Bad Guys	Bad Guys 101 article
Home Networking	Building a Secure Home Environment article Getting Connected article
Home PC Protection	Building a Secure Home Environment article Erasing Files article Home PC Protection presentation Patches and Updates article
ID Theft	Breach Response Notification presentation Introduction to Identity Theft presentation
ISPO's Views (Editorials)	When Online, Free Isn't Always Free Passwords, Facebook, and Apps eMail Tax Scams
Mobile Device Protection	Mobile Device Security presentation Securing Electronic Devices article
Network Security	Network Security presentation
Passwords	Password Cracking 101 presentation
Patching	Home PC Protection presentation Patches and Updates article Scary Internet Stuff presentation
Phishing, Fraud, and Scams	Phishing presentation Scams and Fraud presentation
Privacy	Introduction to Privacy presentation
Security	Introduction to Security presentation
Social Networking	Introduction to Social Media article Safer Social Networking article Safer Social Networking presentation Social Networking Risks article Safer Social Networking 2013 presentation
Viruses and Other Malware	Home PC Protection presentation Introduction to Malware article Scary Internet Stuff presentation

More Cowbell
(Supplemental Info)

CIA's Facebook Program

- CIA's "Facebook" Program Dramatically Cut Agency's Costs
  - http://www.youtube.com/watch?v=ZJ380SHZvYU

Think Before You Post

- Teen Alexa takes a picture of her brother as he sits on the family jet, devouring a Ritz-worthy buffet on their way to Fiji
  - She posts it on Instagram and points to it via her Twitter account
- On the same Twitter account, Alexa happily details her every move
  - The exact days she would arrive in, say, New York
  - Where she was shopping
  - High school graduation dinner invitation that foretold where (time, date, location) her dad and his wife would be in a couple of weeks' time
- Dad is Michael Dell, head of Dell Computers
- He pays about $2.7 million a year for the security protection of his family
  - They shut down Alexa's Twitter account

Systems Track Us Everywhere

- Information about your location is collected *pervasively*, *silently*, and *cheaply*
  - Free Wi-Fi with ads for businesses near the network access point you're using
  - Services telling you when your friends are nearby
  - Electronic tolling devices
    - (FastTrak, EZpass, congestion pricing)
  - Swipe cards
    - Garage / building / door access
    - Monthly transit
  - Parking meters that send you a text when the meter is low
  - Cellphones
  - Surveillance cameras

Where Did You Go?
How would you feel if somebody knew?

- Did you go to an anti-war rally on Tuesday?
- A small meeting to plan the rally the week before?
- At the house of one "Bob Jackson"?
- Did you walk into an abortion clinic?
- Did you see an AIDS counselor?
- Have you been checking into a motel at lunchtimes?
  - Why was your secretary with you?
- Were you the person who anonymously tipped off safety regulators about the rusty machines?
- Were you really home sick Monday?
- Which church do you attend? Which mosque? Which gay bars?
- Who is my ex-husband going to dinner with?

Snooping Technology

- Verizon's attempt -- unsuccessful so far -- to secure a patent for a so-called 'snooping technology,' which in this case would let television advertisers target individual viewers based on what they're doing or saying in front of their sets, capped another challenging year for privacy advocates.
- **Verizon's snooping technology and TV ads**
- The Verizon technology, which includes a sensor/camera housed in a set-top box, would determine the activities of individual viewers -- eating, playing, cuddling, laughing, singing, fighting or gesturing -- and then trigger personal advertisements based on the activities.
- Overall, the technology would serve targeted ads based on what the user is doing, who the user is, his or her surroundings, and any other suitable personal information, according to Verizon.
- The U.S. Patent Office delivered a "non-final" rejection of Verizon's application in November.
- But analysts say that because engineers are already working on such technology, it's a cinch that some kind of similar technology will be included in TV set-top boxes in the not too distant future.

Credit Score + Social Media Mining = Scary

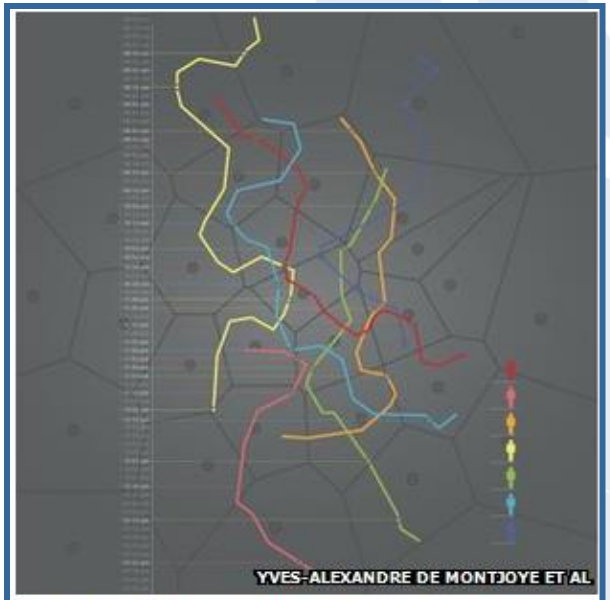
- Financial institutions have started exploring ways to use data from Facebook, Twitter and other networks to round out an individual borrower's risk profile
  - Banks are already using social media to befriend their customers, and increasingly, their customers' friends
- If you are a profitable customer for a bank, a lot of your friends are going to be the same credit profile
- Submitting your Twitter handle will first be pitched as a way to provide customer support or account alerts, which will later open the door for "more complex products"
- If banks learn how to use social media, they could gather information they aren't allowed to ask for on a credit application, including race, marital status and receipt of public assistance

Some Data Mining Correlations

- A prospective insurance policyholder with numerous speeding tickets is more likely than a safer driver to end up with a sports injury
- People who frequent ATMs so they can make cash payments tend to live longer than those who prefer writing checks or paying with credit cards
  - Why? Theory is that ATM users tend to be more spontaneous types, who like to have cash in their pocket and whose lifestyle may be more active
- People with long commutes tend to die younger
  - Why? Theory is that sedentary commutes mean less time to do something healthy in the evening

Location Data Creates “Fundamental Constraints” on Privacy

- Scientists say it is remarkably easy to identify a mobile phone user from just a few pieces of location information
  - Patterns of human movement are predictable enough to identify a specific smartphone user from four data points
- Researchers at MIT and the Catholic University of Louvain studied 15 months’ worth of anonymized mobile phone records for 1.5 million individuals
- “The way we move and the behavior is so unique that four points are enough to identify 95% of people”



The fairly predictable nature of human movement makes location data more unique to a given user

GPS Routes through Retail-Heavy Roads

- IBM's "smarter traffic" division patents
  - Encourage drivers to take different routes that bring them past certain retail establishments
  - Charge bad drivers a toll for behavior like tailgating
- Goal is to earn fees by monitoring driver activity
- "*By focusing on optimal route determination, the known route planning systems fail to consider non-optimal routes whose presentation to travelers may have value to other parties*."
- In other words, your GPS may route you past Starbucks or McDonalds

GPS tracker in candy

- Nestle is using GPS inside its candy bars to track its customers.
- The candy company launched the “We Will Find You” campaign in the United Kingdom where GPS tracking devices were placed inside six candy bars. Once the winning candy bar wrapper is opened, the tracking device will go off and Nestle officials will be able to find the exact location of the customer.
- “This will alert a secret control room who will scramble a crack team of highly trained individuals,” the commercial states. “They will board a helicopter, find the special bar and give the owner 10,000 pounds ($16,145).”
- The six tracking devices will be placed in Kit-Kat, Aero and Yorkie bars in the U.K.
- CNET reports that Nestle put up 3,000 posters to help promote the contest.
- According to Ad Week, Nestle believes the promotion “will particularly appeal to men.”

Memoto Lifelogging Camera

- This roughly inch and a half square box clips onto your clothes using a sturdy stainless steel clip, and shoots one 5 megapixel, geotagged photo every 30 seconds, storing it on built-in memory that holds up to 4,000 pictures. A built-in accelerometer keeps it from nabbing shots of your desk or nightstand when you take it off, and when you plug it in all your photos are automatically uploaded and securely stored on Memoto's cloud servers for easy viewing via
- “Outsources” your memory a
to events

Disney + Facial Regcognition

- A software engineer visited Disneyland and went on a ride
- Disney offered him the photo of himself and his girlfriend to buy – with his credit card information already linked to it
  - He had never entered his name or information into anything at the theme park
  - Never indicated that he wanted a photo
  - Never alerted the humans at the ride to who he and his girlfriend were
- Based on his professional experience, he said the system had to be using facial recognition technology
  - He had never signed an agreement allowing them to do so, and he declared that this use was illegal

Google's Inactive Account Manager

- You can tell Google what to do with your Gmail messages and data from several other Google services if your account becomes inactive for any reason
  - Launched April 11
  - For managing data after you die
- You can choose to have your data deleted
  - After three, six, nine or 12 months of inactivity
- You can select trusted contacts to receive data from Google's services
  - +1s; Blogger; Contacts and Circles; Drive; Gmail; Google+ Profiles, Pages and Streams; Picasa Web Albums; Google Voice and YouTube

ALL

4 Things ~~your kid's~~ apps might do — but might **not** tell you*

1 They might **collect** and **share** personal info

59% share personal info

11% tell you so

2 They might let your kids spend **real money** — even if the app is free

84% of kids' apps that allow purchases within the app are **free** to download

100 RINGTONES!

3 They might include **ads**

58% include ads

9% tell you so

4 They might link to **social media**

22% link to social media

9% tell you so

* Based on *Mobile Apps for Kids: Disclosures Still Not Making the Grade* at ftc.gov.

What You Can Do

At the online app store

Look at screen shots

Follow a link to read about the developer

Read the description, content rating, and user reviews

On your couch

Download and play the app with your kids

Talk to your kids about your rules for using apps

On your phone or tablet

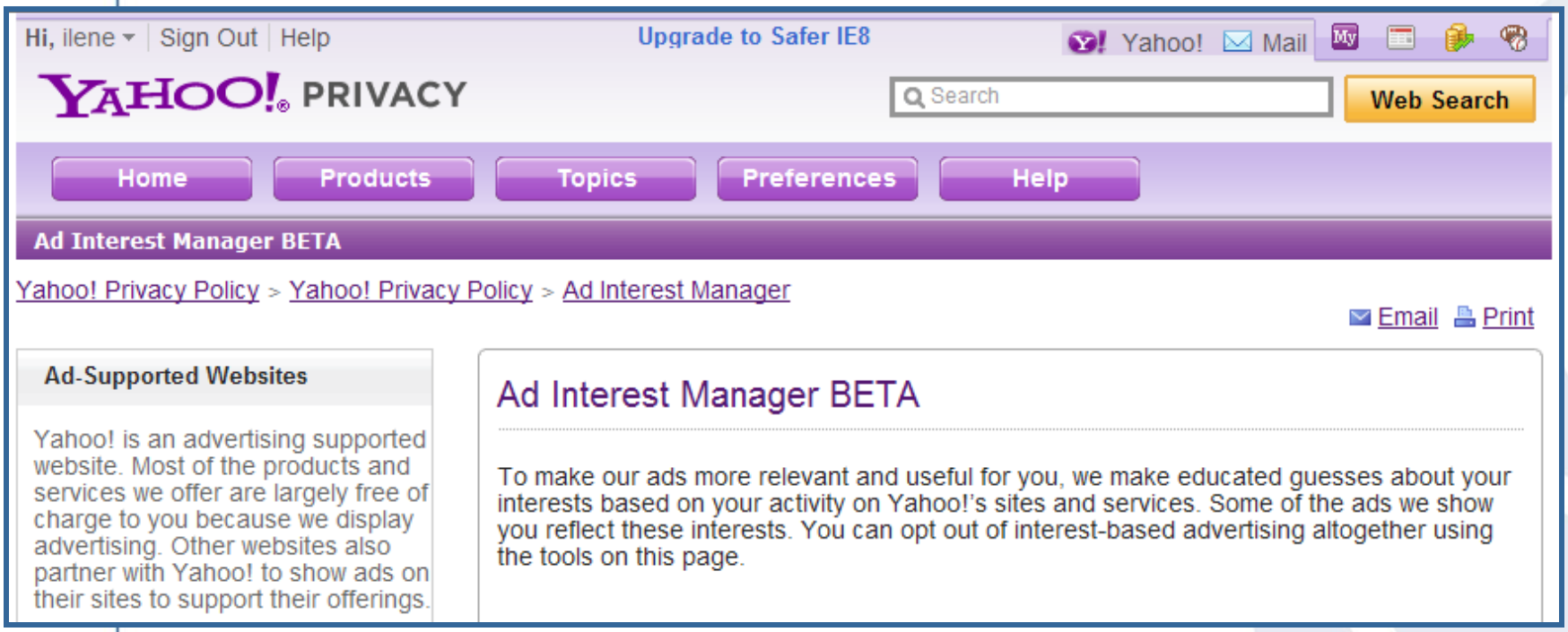
Change your settings, if your phone or tablet allows it

- Restrict content to what's right for your kid's age
- Set a password so apps can't be downloaded without it
- Set a password so your kids can't buy stuff without it

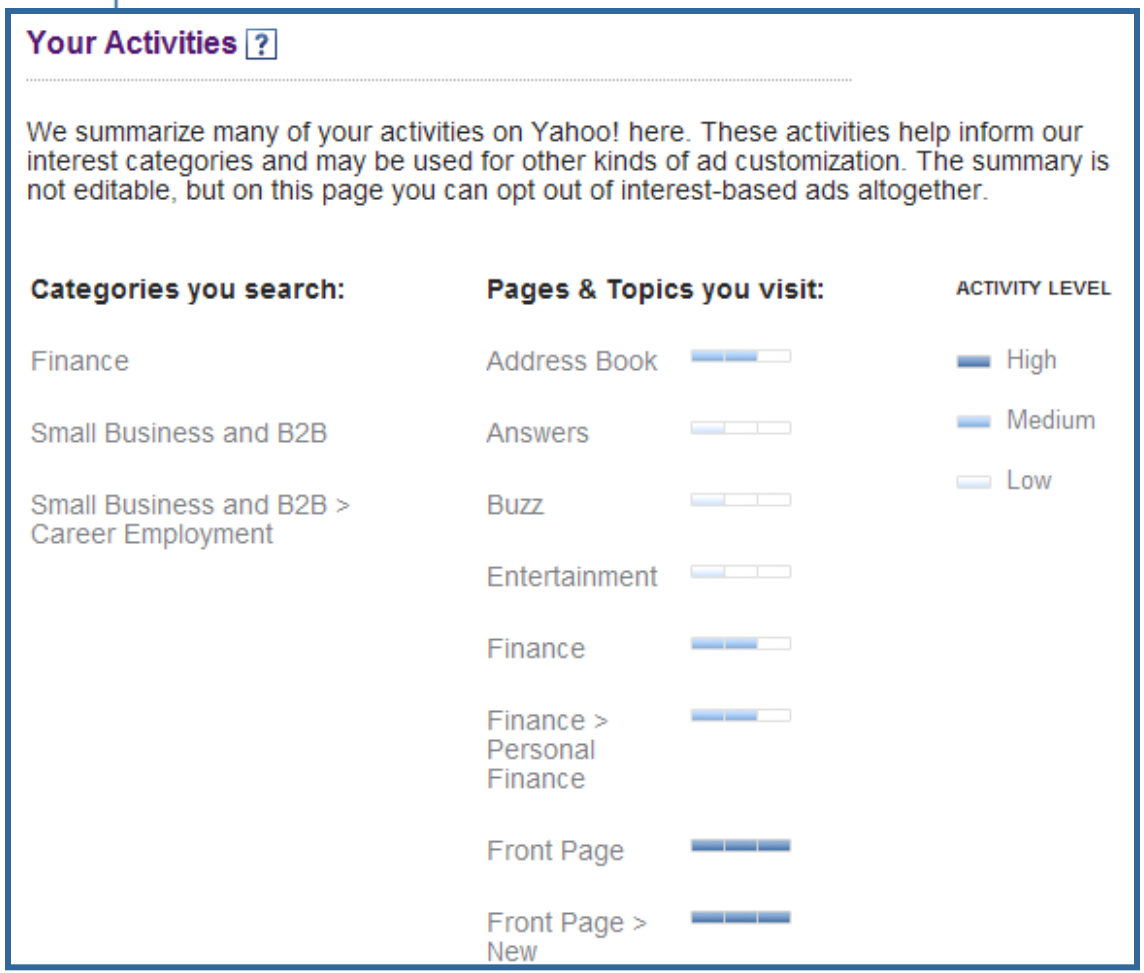
Search for outside reviews of the app from sources you respect

Turn off Wi-Fi and data services or put your phone on airplane mode so it can't connect to the internet

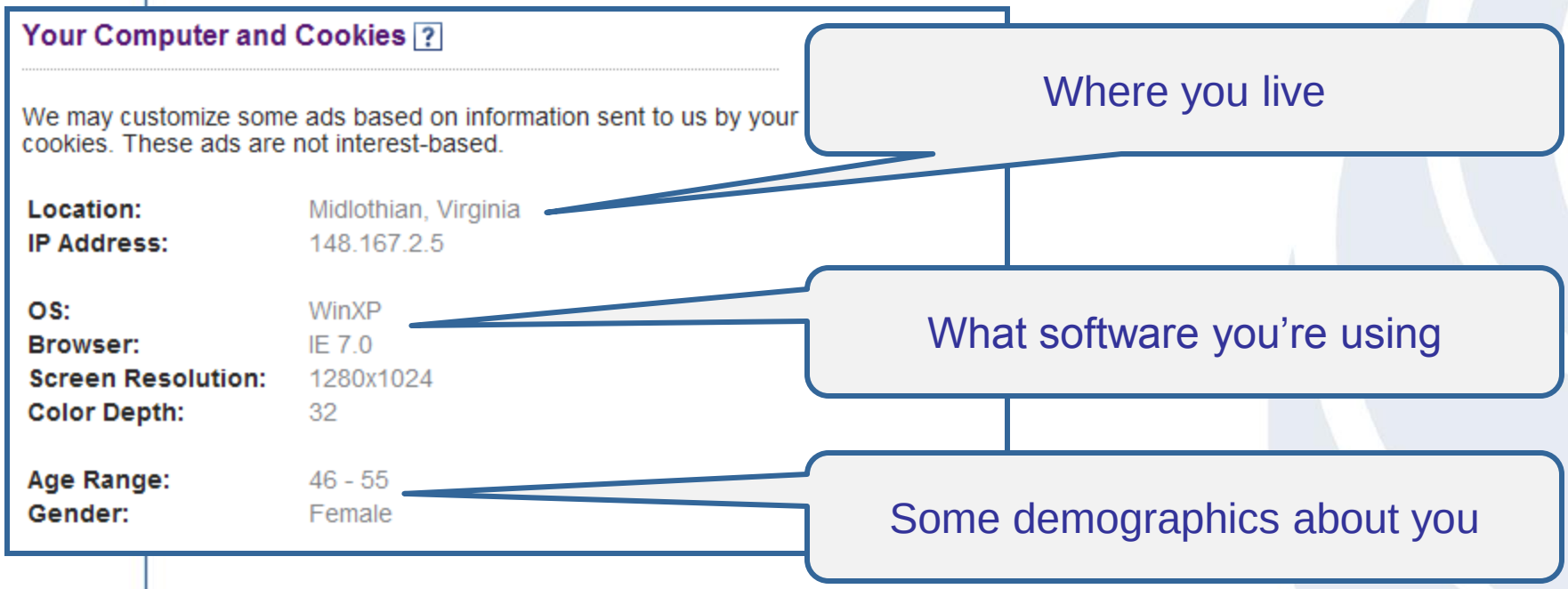
Example: Yahoo Tracks Your Interests



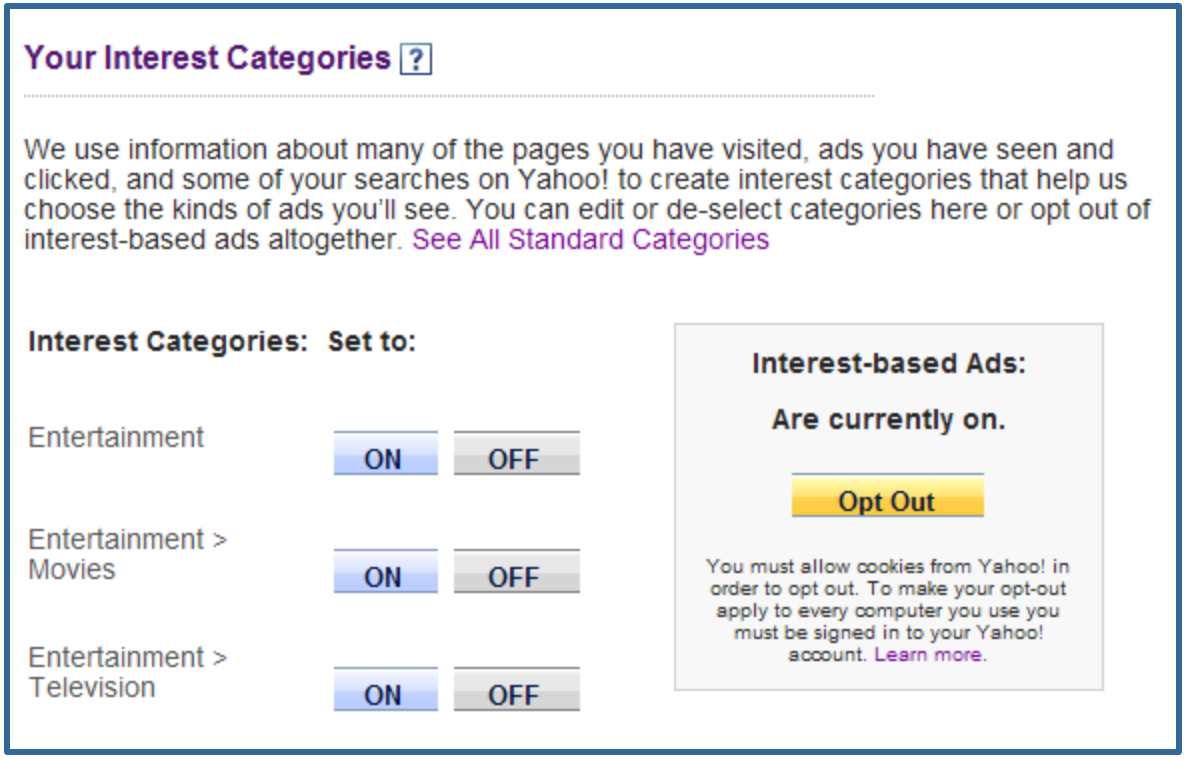
Here Are Some Examples



Yahoo Also Knows



Example: Yahoo Opt Out



FTC Is Our Friend

- The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them
- They’re our protection if a company violates its stated privacy policies

California's "Right to Know" Data Access Bill

- The EU data privacy directive allows its citizens the right to get all data a company holds on them in order to ensure that such data is up to date and correct
- The US does not have that right
- California Assembly Member Bonnie Lowenthal has introduced a bill that may force companies operating in the state to follow EU-style data and privacy rules
  - EFF and ACLU lobbied for the bill
- If passed, the bill will have a significant impact on major Silicon Valley-based companies
  - Including Facebook, Twitter, Google, and other companies that offer Web services
- They're expected to fight the bill

“Do Not Track” Wars

- Microsoft’s IE 10 browser will have “do not track” turned on by default
  - It enraged many online ad companies and industry groups, who see it as overly aggressive and a threat to their business model
- The World Wide Web Consortium says “do not track” controls should not be set by default
  - Internet users would have to provide their “explicit consent” to activate them
  - W3C is responsible for ensuring that web technology is based on an agreed set of technical standards
- So IE 10 would be out of compliance with web standards
- Do Not Track doesn’t attempt to block cookies — instead it is a browser setting that sends a message to every website you visit saying you prefer not to be tracked

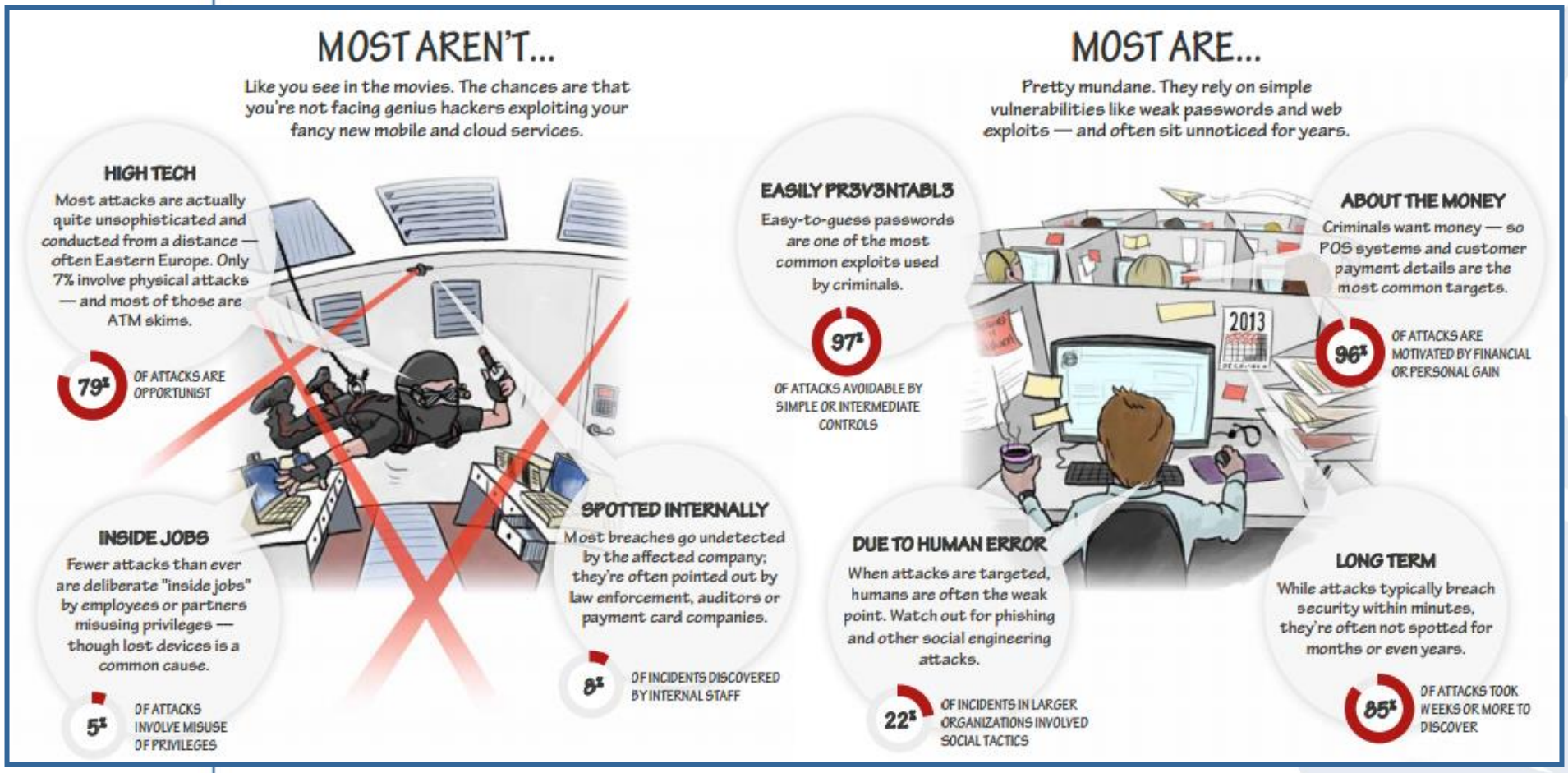
Privacy Hero: Librarians

- Librarians feel a professional responsibility to protect the right to search for information free from surveillance. Privacy has long been the cornerstone of library services in America. Why? Because the freedom to read and receive ideas anonymously is at the heart of individual liberty in a democracy. Librarians defend that freedom every day
- See http://www.privacyrevolution.org/

Raise a Ruckus

- December 18, 2012: Instagram announces changes to terms of service that will allow the company to use pictures in advertisements without notifying or compensating users, and to disclose user data to Facebook and to advertisers
- Users and privacy organizations raised a ruckus
- December 21, 2012: Instagram retreats on changes to terms of service due to user opposition
  - Instagram will “complete our plans, and then come back to our users and explain how we would like for our advertising business to work”

The Truth about Data Breaches



- Source: Verizon Data Breach Report, 2004–2012

Privacy Resources on the Internet

- Privacy Resources and Sites on the Internet is a comprehensive list of privacy resources currently available on the Internet
  - Includes associations, indexes, search engines, individual websites, and sources that supply the latest technology and information about privacy and how it relates to you and the Internet

- http://www.PrivacyResources.info/

Security vs. Privacy

- ***You must implement security to ensure privacy***
  - You must use security to obtain privacy
- Security is technical … privacy is business
- Security is a process … privacy is a consequence
- Security is the sealed envelope … privacy is the successful delivery of the message inside the envelope