

# Data Privacy: Hackers and Headlines



Ilene Klein, CISSP, CISM, CIPP/US  
January 2014



# Agenda

- Your information has been breached –  
Now what?
  - Target hack
- ID theft
- Data brokers and what they know about you
- Privacy and security considerations for the Internet of Things

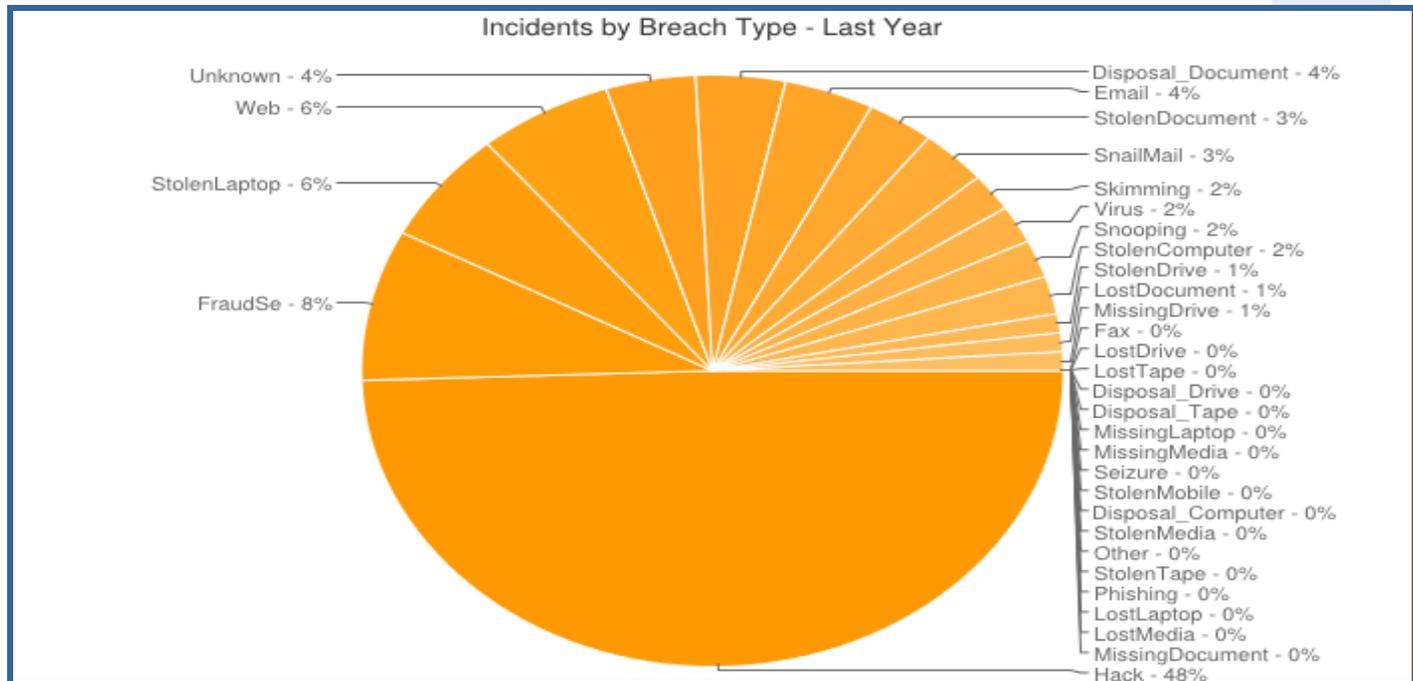






# Congratulations...

- The Target retail store breach affected about 1 in 3 Americans
  - 110,000,000 people
- 1392 breach incidents in 2013
  - Over 740,000,000 records lost worldwide





# Target Breach – What We Know

- The malware used is nearly identical to a piece of malware sold on underground cybercrime forums
  - Costs for \$1,800 (basic version) or \$2,300 (full version)
- Malware name is BlackPOS aka Kaptoxa
  - AV solutions didn't detect it (at the time of the breach)
- The POS malware works by scraping the card data from the POS device's memory (RAM) as soon as the card is swiped
  - Takes advantage of the milliseconds after you swipe your card when your information is not encrypted
- The author of the malware is Russian
- Neiman Marcus and at least three other retailers were also hacked around the same time



# Target Breach – What We Know

- Attackers broke in to Target after compromising a company Web server
  - The attackers had access to Target's network for a while
- Somehow, attackers were able to upload the malicious POS software to store point-of-sale machines
  - They set up a control server within Target's internal network to hold the data collected by all of the infected point-of-sale devices
- Bad guys would keep logging in to that control server and manually collect the dumps (card info)
- They then sold the card data on the black market
  - One bank bought their card data back



# Your Info Has Been Breached

- **NOW What?**



# Your Info Has Been Breached

- **NOW What?**





# Your Info Has Been Breached

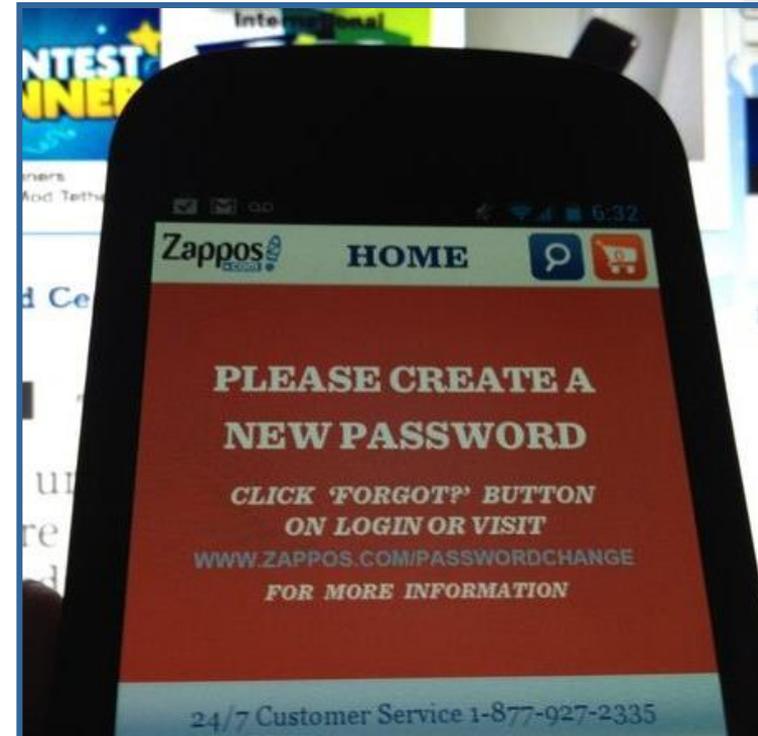
- **NOW What?**





# What Was Breached? Name, Address, eMail

- Be aware
  - You may be a phishing target
- Monitor your finances
  - Bank statements
  - Credit card statements
  - **Low risk of fraud**
- Change your passwords
  - Use different passwords for different accounts





# What Was Breached?

## Credit Card

- Close accounts immediately
  - Call card issuer
- Be aware
  - Look for small purchases (\$1.00 or less) to test if the card is good
- Most card issuers use anti-fraud systems to detect fraudulent use almost immediately
- By calling immediately, you limit your liability for fraudulent charges (to \$50)
- **Credit card fraud ≠ ID theft**





# What Can Thieves Do with Your Info?

- What can thieves really net from your email address, home address, phone number or a credit card number?
- Greatest risk to you is from using the stolen info to make messages seem more legitimate to get you to click
  - Phishing
  - Spear phishing
  - Vishing – phishing via phone calls (voice)
  - Smishing – phishing via text messages (SMS)
- We always need to be vigilant when it comes our information



# Scams after Target Breach

- Bad guys are using the Target breach to scam consumers
- One widely sent text message claimed the recipient's Visa card had been blocked "due to fraud" and asked shoppers to call an 804 telephone number
- Other people have received calls and emails "from someone who said they were with Target asking for my Social Security number and other personal information"



# What Was Breached?

## SSN

- Be aware
- Monitor your credit report
  - Inquiries from companies you didn't contact, accounts you didn't open, debts you can't explain
- Consider placing an initial fraud alert on your credit report
  - Stays on credit report for 90 days
  - Requires businesses to verify your identity before issuing you credit
    - May cause delays if you're trying to obtain credit
- Most organizations will provide 1 year of credit monitoring services
- **Check out [ftc.gov/idtheft](https://www.ftc.gov/idtheft) for resources**



# Medical Records

- Have you ever checked your medical records for accuracy?
    - Blood type
    - Allergies
    - Conditions
    - Major illnesses
    - Hospitalizations
    - Broken bones
    - Medications
- Can kill you if wrong**





# Medical ID Theft

- Medical identity theft has been called the privacy crime that can kill
- Medical identity theft occurs when a person uses someone else's personal information to obtain medical goods and services
  - Receiving medical care using another's information
  - Doctors writing fraudulent prescriptions
  - Having bills sent to another individual
- About 1.8 million people in the U.S. are currently affected by medical identity theft
  - Source: 2013 Survey of Medical Identity Theft conducted by the Ponemon Institute



# Medical ID Theft

- **Victims usually know the perpetrator!**
- 30% of survey respondents knowingly permitted a family member to use their personal identification to obtain medical services
  - Including treatment, healthcare products, or pharmaceuticals
- 28% said a member of the family took their personal identification or medical credentials without consent



# Medical ID Theft Detection and Prevention

- Review the Explanations of Benefits carefully
- Review your medical records
- Monitor your credit reports
- Shred confidential documents
- Review the Medical ID Theft tip sheet
  - On [phoenix.gov/infosec](http://phoenix.gov/infosec)
- Ask your health care providers about their security and privacy practices
  - Give your health care providers the Medical ID Theft recommendations (on [phoenix.gov/infosec](http://phoenix.gov/infosec))



**First Aid**  
For Medical Identity Theft  
*Tips for Consumers*

Consumer Information Sheet 16 • October 2013

## Medical Identity Theft

Recommendations for the Age of Electronic Medical Records



# Identity Thieves Steal Tax Refunds

- Bad guys with your social security number use fake information and file tax returns in your name to get your refund
  - They print fake W-2 forms and other docs
- In 2010, about 15 percent of all identity theft complaints to the FTC dealt with tax returns. In 2013, that jumped to 43 percent.
- **File early!**
  - **Goal is to beat the thieves**
- Indicator is that you get a message from the IRS that you've already filed your return
  - IRS says a typical case can take about 180 days to resolve. They're working to identify fraudulent returns



# Who Has Your Data?

- Think of all the businesses and other entities that have your personal information stored in their databases
  - City, county, state, and federal government organizations, probably many at each level
  - Every credit card, bank and financial account provider
  - Any online merchant with whom you've set up an account
  - Schools, discussion forums, social media, doctors, dentists, hobby groups, magazine companies, travel agencies...





# Data Brokers (1)

- Data brokers: Companies that track our every move and then sell private details about our personalities to businesses
- Brokers are amassing a huge amount of detailed private data on consumers without their knowledge
- They're a **\$156 billion** industry
- The Senate commerce committee and the FTC have been investigating them

Out of the 2,397 data broker companies, Acxiom Corporation is known as “the quiet giant.”

It has the world's largest commercial consumer database, with information about

**500 million**  
active consumers worldwide.

Acxiom's database is so extensive that it had data on

**11 of the 19**  
9/11 hijackers.



# Data Brokers (2)

- Just say “no” when a cashier asks for your zip code

## Where do they get this data?

There are three primary types of sources:



### Public

Government records, public records, publicly available data



### Volunteered

Self-reported data from surveys and questionnaires



### Private

Mostly data from other commercial entities, employers, online trackers

Axiom uses a shopper recognition program that cross-references a customer's ZIP code or phone number with a name from a check or credit card to confirm shopper identities within a 10 percent margin of error  
--and they never have to ask permission.

## How are data brokers used?

Companies and organizations in the U.S. spend more than \$2 billion a year on third-party data

Why? In short: to sell you things, but also:



information research



identity verification



fraud prevention



background checks



# Data Brokers (3)

- Data brokers take knowledge about us and lump us into buckets
  - Example: Describing our financial situation

<b>"Burdened by Debt: Singles"</b>	<b>"Struggling Elders: Singles"</b>	<b>"Meager Metro Means"</b>	<b>"Very Elderly"</b>
<b>"Mid-Life Strugglers: Families"</b>	<b>"Retiring on Empty: Singles"</b>	<b>"Relying on Aid: Retired Singles"</b>	<b>"Rolling the Dice"</b>
<b>"Resilient Renters"</b>	<b>"Tough Start: Young Single Parents"</b>	<b>"Rough Retirement: Small Town and Rural Seniors"</b>	<b>"Fragile Families"</b>
<b>"Very Spartan"</b>	<b>"Living on Loans: Young Urban Single Parents"</b>	<b>"Financial Challenges"</b>	<b>"Small Town Shallow Pockets"</b>
<b>"X-tra Needy"</b>	<b>"Credit Crunched: City Families"</b>	<b>"Credit Reliant"</b>	<b>"Ethnic Second-City Strugglers"</b>
<b>"Zero Mobility"</b>		<b>"Rocky Road"</b>	<b>"Rural and Barely Making It"</b>
<b>"Hard Times"</b>			
<b>"Enduring Hardships"</b>			
<b>"Humble Beginnings"</b>			



# So What's Your Bucket?

- OfficeMax sent a marketing letter addressed to a man, but the second line read “Daughter Killed in Car Crash”
  - Man’s 17-year-old daughter was killed in a crash last April when the SUV veered off the road and slammed into a tree
- OfficeMax apologized and said
  - “...This mailing is a result of a mailing list rented through a third-party provider...”
- **A father loses his daughter and that’s how OfficeMax or its provider chose to market to them**



# Axiom's About the Data

- What does one of the largest data brokers know about you?
- Visit [Axiom's AboutTheData.com](http://Axiom'sAboutTheData.com)

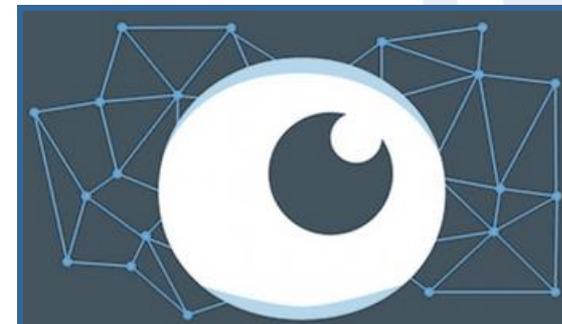
Averaging about  
**1,500**  
data points *apiece*,  
each consumer is  
assigned a 13-digit code  
and placed in one of  
**7,018**  
detailed socioeconomic  
clusters.



Their commercial  
consumer database  
contains "nearly  
every U.S. consumer,"  
with data on

**126 million**  
U.S. households and

**190 million**  
individuals.



The company combines its 43-year-old  
offline database with mobile activity  
and online data from  
**75,000**  
websites annually to create what's called a  
"360-degree view" of consumer behavior.



# Example Data – From a Real Person

- Inaccurate data is flagged



Element	Details	Action
Date of Birth	 09/03/1967	 Edit/Remove
Age Range	 Age 46 -47	 Edit/Remove
Gender	 Male	 Edit/Remove
Race	 White	 Edit/Remove
Marital Status	 Married	 Edit/Remove
Political Party	 Voter - Republican	 Edit/Remove
Occupation	 Professional/Technical	 Edit/Remove
SOHO Indicator	 True	 Edit/Remove

Element	Details	Action
Auto Policy Renewal Month	 July	 Edit/Remove
Intent to Purchase a Vehicle	 True	 Edit/Remove



# Example Data – From a Real Person

Element		Details	Action
Estimated Household Income Ranges 1	▲ ?	\$20,000 - \$29,999	<a href="#">Edit/Remove</a>
Estimated Household Income Range	▲ ?	\$25,000 - \$29,999	<a href="#">Edit/Remove</a>
Life Insurance Policy Owner	?	True	<a href="#">Edit/Remove</a>
Presence of Credit Card	▲ ?	Bank Card Holder, Gas/Department/Retail Card Holder, Credit Card Holder - Unknown Type, Premium Card Holder	<a href="#">Edit/Remove</a>
Credit Card Use - MasterCard	▲ ?	Regular	<a href="#">Edit/Remove</a>
Online Purchasing Activity	?	True	<a href="#">Edit/Remove</a>
Number of Purchases - Credit Card	?	1	<a href="#">Edit/Remove</a>
Number of Purchases - MasterCard	?	4	<a href="#">Edit/Remove</a>
Number of Purchases - Other	?	3	<a href="#">Edit/Remove</a>

▲ ? **\$20,000 - \$29,999**

Estimated household income from all household members. Sources: Surveys, Public Data, Online/Offline Registrations, Magazine Subscriptions Warranties, Retail Buying Activity



# Example Data – From a Real Person

Element		Details	Action
Mail Order Responder	?	<b>Mail Order Responder</b>	<a href="#">Edit/Remove</a>
Mail Order Buyer	?	<b>Mail Order Buyer</b>	<a href="#">Edit/Remove</a>
Food/Beverages Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Travel	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Arts and Antiques	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Computing/ Home Office - General	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Pet Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Women's Apparel	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Women's Plus Sizes Apparel	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Holiday/Ethnic Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Health and Beauty Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Gardening Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Home and Garden Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Home Furnishings Accessories	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Golf Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Sports and Leisure Products	?	<b>Purchased</b>	<a href="#">Edit/Remove</a>
Total Dollars Spent	?	<b>447</b>	<a href="#">Edit/Remove</a>
Total Number of Purchases	?	<b>8</b>	<a href="#">Edit/Remove</a>
Average Dollars Spent Per Offline Purchase	?	<b>75</b>	<a href="#">Edit/Remove</a>
Total Offline Dollars Spent	?	<b>150</b>	<a href="#">Edit/Remove</a>
Total Number of Offline Purchases	?	<b>2</b>	<a href="#">Edit/Remove</a>
Total Offline Purchases - Under \$50	?	<b>1</b>	<a href="#">Edit/Remove</a>



# Example Data – From a Real Person

Element	Details	Action
Beauty/Cosmetics	? Interested	<a href="#">Edit/Remove</a>
Financially Support Community Causes	? Animal Welfare, Health, Veteran's	<a href="#">Edit/Remove</a>
Community/Charities	? Interested	<a href="#">Edit/Remove</a>
Wireless Product Buyer	? Interested	<a href="#">Edit/Remove</a>
Computers	? Interested	<a href="#">Edit/Remove</a>
PC Internet/Online Service User	? Interested	
PC Modem Owner	? Interested	
Wireless - Cellular Phone Owner	? Interested	
Consumer Electronics	? Interested	
PC DSL/High-Speed User	? PC Broadband User	
Arts	? Interested	
Home Stereo	? Interested	
Avid Music Listener	? Interested	
Movies at Home	? Interested	
Casinos	? Interested	
Sweepstakes/Contests	? Interested	
Cooking	? Interested	
Gourmet Cooking	? Interested	
Low-Fat Cooking	? Interested	

Cholesterol - Related Products	? Interested	<a href="#">Edit/Remove</a>
Health/Medical	? Interested	<a href="#">Edit/Remove</a>
Dieting/Weight-loss	? Interested	<a href="#">Edit/Remove</a>
Current Affairs/Politics	? Interested	<a href="#">Edit/Remove</a>
Music Players	? Interested	<a href="#">Edit/Remove</a>
Collecting	? Interested	<a href="#">Edit/Remove</a>
Collectible Antiques	? Interested	<a href="#">Edit/Remove</a>
Home Furnishings/Decorating	? Interested	<a href="#">Edit/Remove</a>
Home Improvement	? Interested	<a href="#">Edit/Remove</a>
Gardening	? Interested	<a href="#">Edit/Remove</a>
Personal Investment	? Interested	<a href="#">Edit/Remove</a>
Stocks/Bonds Investment	? Interested	<a href="#">Edit/Remove</a>
Dog Ownership	? Interested	<a href="#">Edit/Remove</a>
Other Pet Ownership	? Interested	<a href="#">Edit/Remove</a>
Reading	? Interested	<a href="#">Edit/Remove</a>
Reading Magazines	? Interested	<a href="#">Edit/Remove</a>
International Vacation	? Have Taken	<a href="#">Edit/Remove</a>
Domestic Travel	? Interested	<a href="#">Edit/Remove</a>
International Travel	? Interested	<a href="#">Edit/Remove</a>



# StopDataMining.me

- StopDataMining.me is a master list of opt-out links to stop data brokers from collecting information about your online and offline activities

## Master List of Data Broker Opt-Out Links

Now tracking 50 data mining companies.

Show  entries

Search:

CATEGORY ⇅	COMPANY NAME ⇅	OPT-OUT LINK ⇅	METHOD ⇅	NOTES
TOP 10	Acxiom Corporation (NSDQ:AXCM)	<a href="https://isapps.acxiom.com/optout/optout.aspx">https://isapps.acxiom.com/optout/optout.aspx</a>	Online Form / Mail / Telephone	Complete a request on valid email Telephone 2094, and :
TOP 10	DataLogix Holdings, Inc.	<a href="https://www.datalogix.com/privacy/#opt-out-landing">https://www.datalogix.com/privacy/#opt-out-landing</a>	Online Form	Fill out onli



# Did Facebook Raise Your Interest Rate

- More lending companies are mining Facebook, Twitter and other social-media data to help determine a borrower's creditworthiness or identity
  - Does a job applicant put the same job information on their loan application as they post on LinkedIn
  - Did they shared on Facebook that they had been let go by an employer
  - Does a small business have negative reviews on eBay
- Fair Isaac Corp. (FICO), which provides the credit scoring used in more than 90% of lenders decisions, says it is weighing possibilities for incorporating social media
- Trend is raising concerns among consumer groups and regulators



# Check Your Privacy Settings

- Here's a list of easy instructions to update privacy settings wherever and however you go online
- <http://www.staysafeonline.org/data-privacy-day/check-your-privacy-settings/>



# Helping Victims Control their Digital Footprint

- January 2014: As part of Data Privacy Day, Reputation.com will help survivors of domestic violence and sexual assault control their digital footprint by offering its MyPrivacy™ tool at no charge
  - MyPrivacy removes personally identifiable information from the Internet and helps prevent third parties from accessing Web surfing activities
- The National Cyber Security Alliance is partnering with Reputation.com and the Rape, Abuse & Incest National Network (RAINN) to empower survivors of domestic violence and sexual assault by offering tools and resources that will help survivors gain control of their digital footprint and protect their personal information



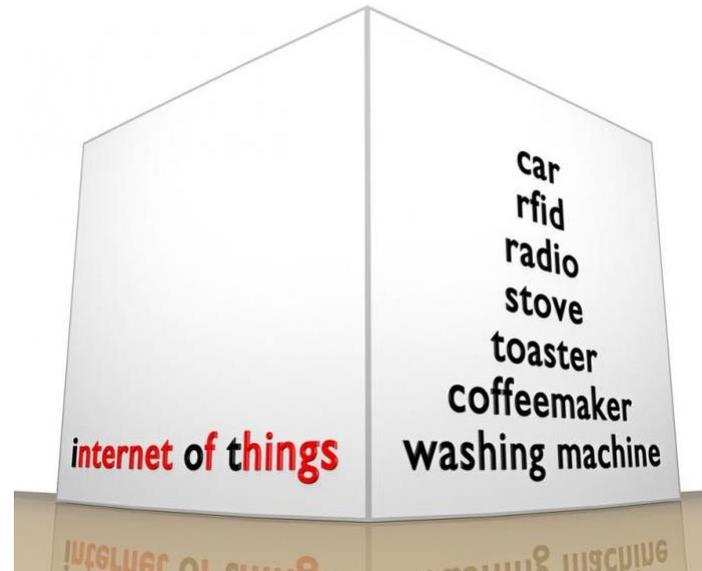
\* Or if you want to make sure your card's not breached, or if you want to make an anonymous purchase



# Internet of Things

- “By 2015, there will be 25 billion things hooked to the Internet. By 2020, that will grow to 50 billion.

In the consumer market, smart devices will track our health, help us remotely monitor an aging family member, reduce our utility bills and tell us we’re out of milk.”





# Brush Smarter

- Use your internet-connected toothbrush!
  - New toothbrush includes a sensor that detects how much tartar is being removed in a brushing
  - It also records brushing activity so users can maintain a consistent cleaning each time
- The device conveys the information wirelessly to a smartphone app
  - The app can tell users if they have missed hard-to-clean areas or are not getting a thorough brushing
  - Let's parents monitor their kids' teeth brushing
- Debuted at CES January 2014





# Internet-Connected Baby Onesie

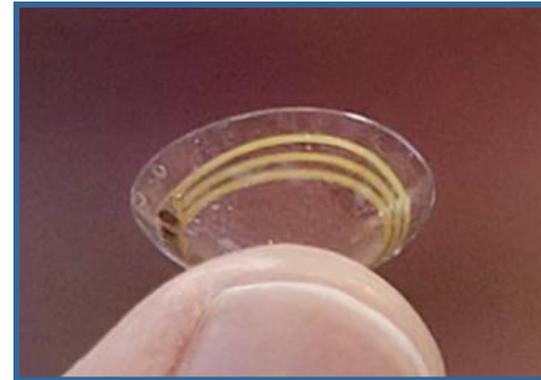
- The Mimo Baby has two green stripes on the front that are respiratory sensors
- The onesie comes with a removable, turtle-shaped clip, with sensors allowing it to monitor the baby's body position, activity level and skin temperature
- Think of this as the baby monitor of the future
- Parents can see all the data in an iOS/Android app





# RFID for Medical “Devices”

- New breast implants come equipped with radio frequency chip to help diagnose problems
- Google is developing a soft contact lens that measures the glucose levels in tears
- Both use RFID to transmit information to monitors





# Connected TVs, Fridge Help Launch Global Cyberattack

- Between December 23 and January 6, more than 750,000 emails were sent from more than 100,000 appliances
  - Included everyday consumer gadgets such as home-networking routers, televisions and at least one “smart” refrigerator
  - About three-quarters of the emails were sent by regular computers, but the rest, slightly more than one-quarter, were sent by hacked home appliances.
  - Hackers usually gained access because the home owners didn’t set them up the devices correctly or used the default password (hackers didn’t have to be too smart)
  - Devices were infected with malware that turned them into spambots
- This is being called possibly the first proven cyberattack to originate from connected appliances, according to security firm, Proofpoint



# Connected TVs, fridge help launch global cyberattack

## Update

- Nope – the fridge did not send out spam
- It just happened to be on the same network as the spambot
  - According to Symantec
- **But it's going to happen**
  - Madam Ilene's prediction



# Your TV Watches You Watch TV

LG promises to stop your Smart TV spying on you

BY MATT BRIAN • NOVEMBER 21ST, 2013 AT 9:38AM ET

- An IT consultant in England got suspicious after he noticed that his new LG smart TV began showing him targeted ads based on programs he'd just been watching
- He discovered every show he watched and every button he pressed on his remote control were being sent back to LG's corporate headquarters in South Korea
  - He used his laptop to monitor wireless traffic between the TV and his Wi-Fi receiver
- Without his knowledge, his TV had sent the contents of private videos he'd watched on the TV, including camcorder footage of family celebrations of his wife and two young children
  - TV continued sending such information to Korea even after he adjusted the television's default settings to "opt out" of data sharing



# IoT Security and Privacy

- Devices need security and privacy built into them
- Most security and privacy professionals think it will take a high-profile, catastrophic hack of smart consumer devices to force the market to address security of those products
- FTC is looking into security and privacy of devices





# Thinking of Buying an Internet Thing?

## What to Ask (1)

- You may not understand the answers (or even get any)
  - Remember the first time you bought a PC?
- Pay attention to **how** the salesperson answers
- Red flags
  - Blank stare
  - Too “glib” a response (“our product is 100% secure and guarantees your privacy”)
  - Too much technobabble (“it uses hyper-encryption”)





# Thinking of Buying an Internet Thing?

## What to Ask (2)

- Which of my data does [product name] collect? What does it do with it? Where does it store the data? And how does it protect the data from unauthorized access? Is my data shared?
- Was this product independently audited by an application security expert prior to its release? If so, what kind of testing was performed?
- How does this product protect communications coming and going?



# Thinking of Buying an Internet Thing?

## What to Ask (3)

- Does this product run any third party software (like Java or Webkit)?
  - Makes the product more vulnerable to malware – just like a PC
- What default security features does this device have?
- Are there any default accounts / passwords
  - How do you change the password?
- How do you update the product's software if there's a security vulnerability? Do you have a process to do that?

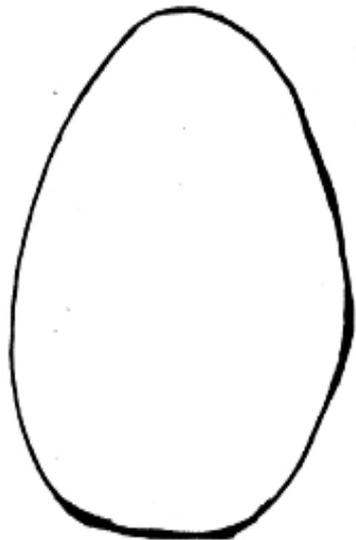


# Key Points

- **Be aware**
  - Privacy is sometimes a trade-off
  - But don't blindly give it up
- **Be aware**
  - Understand how your info will be used and whether it's shared
- **Be aware**
  - Control things that you can control
  - Protect devices, your accounts, and your information



THIS IS YOUR  
PRIVACY.



THIS IS YOUR PRIVACY  
ONLINE.



ANY QUESTIONS?



# More Cowbell (Supplemental Info)

**City of Phoenix**



# Hazards of Social Media

- January 4, 2014: Colts punter Pat McAfee tweeted a picture of Indy's excited locker room to his almost 170,000 followers
  - After the Indianapolis Colts came back from a 38-10 halftime deficit to beat Kansas City 45-44
- Oops – there's a mostly-naked quarterback in the picture
  - Andrew Luck was still getting dressed when McAfee took the photo





# Think You Know Privacy? Take the quiz!

- <http://myprivacyiq.com/>
- (It's easy)



# New Cyber Stalker App

- January 2014: New app coming out for Android and iOS called NameTag
- You upload a snapshot of a person
- App compares it to publicly available social media accounts and dating website profiles
  - It also scans criminal databases, like the National Sex Offender Registry
- Uses facial recognition software
- What results is a detailed dossier of your subject





# Why We Won't Get a Federal Data Breach Notification Law Anytime Soon

- Many politicians have tried to get national data breach notification law
  - Example: Sen. Patrick Leahy of Vermont has introduced the Personal Data Privacy and Security Act every Congress since 2005
- Too many committees say they have jurisdiction over privacy
- The 46 state laws have different
  - Triggers for breach notification (breach vs harm threshold)
  - Required content of notifications
  - Required timeframe for notifications
- Congressional dysfunction and unwillingness to compromise



# Let's Collect Your Phone Signal

- The owner of a trendy Asian restaurant in downtown Toronto knows that 170 of his customers went clubbing in November
- He knows that 250 went to the gym that month, and that 216 came in from Yorkville, an upscale neighborhood
- How? He subscribes to a service that tracks signals emitted from Wi-Fi-enabled smartphones
- The service has created portraits of roughly 2 million people's habits as they have gone about their daily lives, traveling from yoga studios to restaurants, to coffee shops, sports stadiums, hotels, and nightclubs
- Info doesn't include names, but the company does collect the names, ages, genders, and social media profiles of some people who log in with Facebook to a free Wi-Fi service
- Companies don't have to get a consent before collecting and sharing most personal information, including their location.



# GPS Tracking

- On January 8, Ford Vice President Jim Farley said, “We know everyone who breaks the law; we know when you’re doing it. We have GPS in your car, so we know what you’re doing. By the way, we don’t supply that data to anyone.”
- Farley and Ford have since retracted the statement, but Franken says there is evidence that Ford is tracking and supplying personal information to other parties.



## New Google+ “Feature”

- Any Gmail user who is signed up to Google Plus can now email any other Gmail user who is signed up to Google Plus
  - Even if the sender does not know the recipient’s email address
- Basically Google makes it easier for strangers to email you
- You can opt-out
- Privacy professionals have criticized this new “feature”



# A World with Zero Privacy

- How would a world with zero privacy look?
  - Ubiquitous, inescapable collection of personal data
  - Near-perfect predictive capability of that data
  - Mandatory availability of that data
- Privacy Death Index
  - Proposed by Jay Cline, privacy expert

Privacy death index for the U.S., 2001-14

	Ubiquity of data collection		Efficacy of predictive analytics		Pervasiveness of data sharing	
<i>Rating criteria</i>	1: less than comprehensive and mostly voluntary 2: comprehensive and mostly voluntary 3: comprehensive and mandatory		1: highly accurate in some use cases 2: highly accurate in many use cases 3: highly accurate in all important use cases		1: widespread voluntary sharing and some mandatory sharing 2: widespread mandatory sharing with corporations 3: widespread mandatory sharing with governments	
	2001	2014	2001	2014	2001	2014
Health data	1	1	1	1	0	1
Productivity and aptitude data	1	1	1	1	0	0
Consumption and financial data	1	2	1	2	1	2
Behavior and belief data	0	0	0	1	0	1
Social graph	0	1	0	1	0	1
Location data	0	2	0	1	0	1
<b>TOTAL (out of 18 possible)</b>	<b>3</b>	<b>7</b>	<b>3</b>	<b>7</b>	<b>1</b>	<b>6</b>

Source: Jay Cline



# In a Zero-Privacy World: Most Valuable Data About Us

- Health capacity – predicted longevity and strengths and weaknesses in our DNA
  - Used by prospective mates, employers, healthcare providers and insurers
- Productivity capacity – natural aptitudes and predicted earnings potential
  - Used by Match.com users and employers
- Consumption instinct – what we like to buy, how much, when and why, and our credit worthiness
  - Used by marketers (who are already paying for this data) and tax authorities
- Behavior instinct – our public and private statements, beliefs, politics and capacity to act outside social norms
  - Used by national-security, law enforcement agencies, and politicians
- Social graph – past and present family, friends, neighbors, classmates and colleagues
  - Used by marketers, criminals, national security and law enforcement
- Location and predicted movement – where we've gone and will go
  - Used by marketers, the military, and police



Dilbert.com DilbertCartoonist@gmail.com



11-28-13 © 2013 Scott Adams, Inc., Ph.D. by Universal Uclick





# Surveillance Spaulder

- Spaulder – the plating that wraps around your armored shoulder
- Surveillance spaulder – a new device that makes your shoulder twitch whenever it detects a security camera
  - It has sensors that detect the type of infrared lighting commonly used with surveillance cameras and sends an electric signal to two “transcutaneous electrical nerve stimulation” pads





# Encrypt the Web – Who's Doing What

	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
	undetermined	limited	✗	undetermined	✗
	undetermined	✓ (iCloud)	✗	undetermined	✗ (me.com, mac.com)
	undetermined	undetermined	✗	undetermined	✗ (att.net)
	undetermined	undetermined	✗	undetermined	✗ (comcast.net)
	✓	✓	✓	✓	✓
	✓ in progress	✓	✓ planned	✓	✓ (in progress, facebook.com)
	undetermined	✓	✓	undetermined	✗
	✓	✓	in progress for select domains, see notes	✓	✓
	✗ contemplating	✓ planned 2014	✓ planned 2014	✓ planned 2014	✗ contemplating
	✓ in progress	✓	✗	✓ in progress	✗ (outlook.com)



# Microsoft vs Google

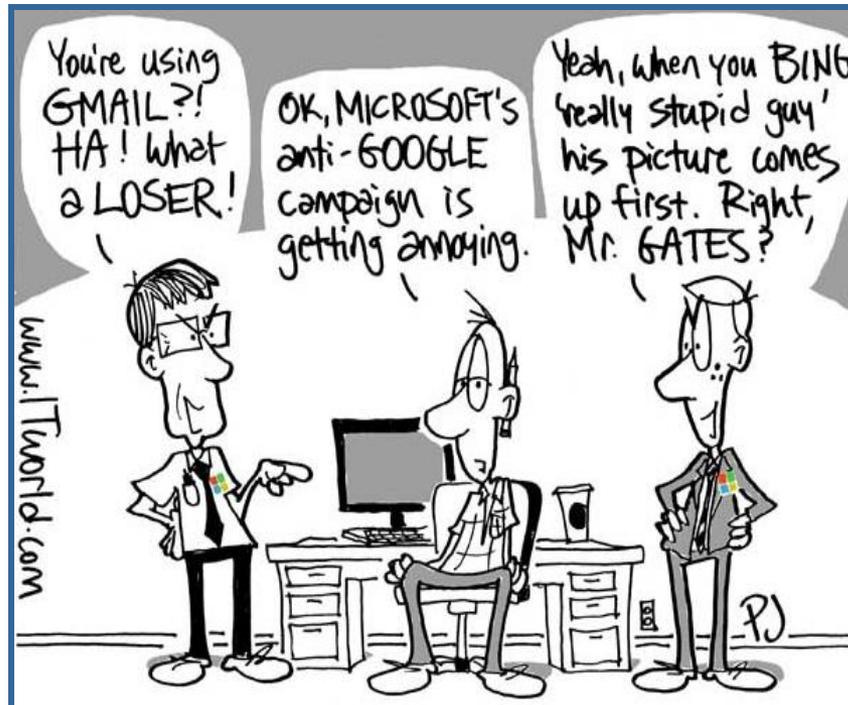
- Microsoft launched a public relations campaign against Google based on its privacy policies
- Industry folks think Bill Gates and company's efforts to get people to stop using Google is getting silly



Scroogled I'm Watching You T-shirt

Do you use Google Search? Or Gmail? Or Google Chat? Or Chrome? Then Google is watching you...all the time.

\$11.99



Scroogled Logo T-shirt

A classic that shows the world that you're tired of having your digital life monetized by Google.

\$11.99



# Track Tracking Cookies

- October 2013: Mozilla released Lightbeam for Firefox, an add-on that lets you track tracking cookies
  - See what companies are behind each cookie and what information they're gathering
- Tracking cookies track browsing history on a single site or network of websites
  - Identify site visitors, and note the frequency and content of visits across a network
  - Browsing history is used to sell ads and serve targeted ads to site visitors



# Top 5 Countries for Privacy

- Top 5
  - Spain
  - Czech Republic
  - Iceland
  - Norway
  - Slovenia
- Bottom 5
  - Bahrain, Iran, Nigeria  
Syria, Malaysia
- Source: [BackgroundChecks.org](http://BackgroundChecks.org)
- Based on country's
  - Privacy laws
  - Internet restrictions
  - Government spyware
  - Free speech protections
  - Other metrics