Protecting Privacy in the Information Tracking Age

What to Know | What to Do

INFORMATION SECURITY & PRIVACY OFFICE

Randell C. Smith, Jr. CISM, CISSP, PMP
Chief Information Security Officer | Chief Privacy Officer
City of Phoenix

Agenda

- Is Privacy Dead in the Information Age?
- Do you have a “Right to be Left Alone?”
- Should Privacy “desires” trump Legal Processes?
- Are you the Customer or the Product?
- What can/should you do?

Background

- 9 years with City of Phoenix
- Serving as CISO and CPO
- 30 years with U.S. Navy (Retired Captain)
- Naval Cryptologist
- Worked directly for Naval Security Group Command and National Security Agency
- Hold multiple industry certifications

The sky is not falling…it's just a little closer!

Charles Thompson, former CIO, City of Phoenix.

Question: Is Privacy Dead in the Information Age?

Facebook's Zuckerberg Says The Age of Privacy is Over

"Facebook founder Mark Zuckerberg told a live audience yesterday that if he were to create Facebook again today, user information would by default be public."

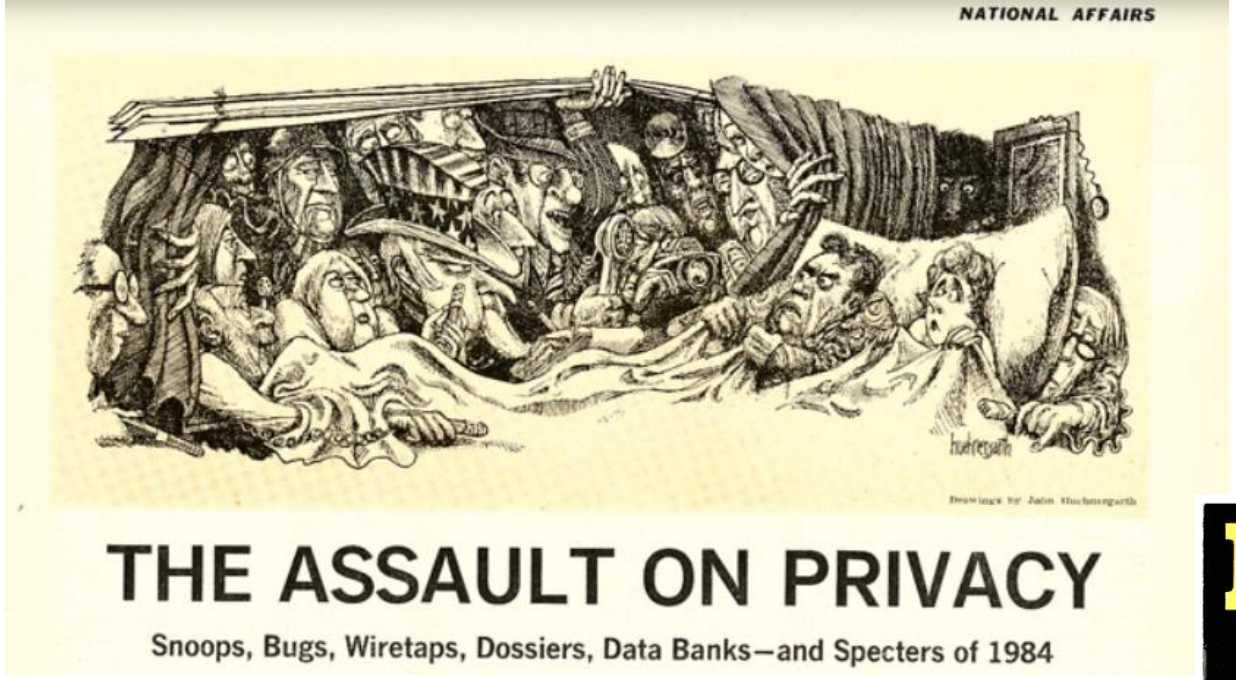
January 9, 2010

LEADERSHIP 8/19/2014 @ 12:04AM | 8,891 views

Privacy Is Completely And Utterly Dead, And We Killed It

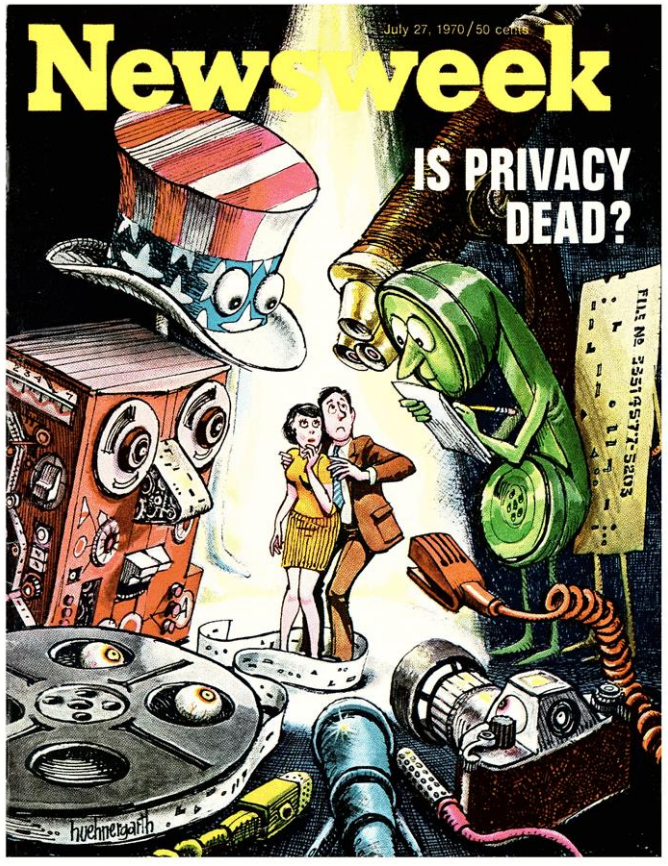
Forbes

January 9, 2010



July 27, 1970

This is not a new concern.



Tom Cruise – Minority Report (2002)

Tom Cruise's character walks through a shopping area as advertisements address him by name. "John Anderton! You could use a Guinness right now," says one affable billboard. "

Advertising Company Will Use Its Billboards To Track Passing Cellphones (March 1, 2016)

- Clear Channel Outdoor will use billboards to map real-world habits and behaviors from nearby consumers.

- "Using anonymous aggregated data from consumer cellular and mobile devices, RADAR measures consumer's real-world travel patterns and behaviors as they move through their day, analyzing data on direction of travel, billboard viewability, and visits to specific destinations."

All data is anonymous and aggregated meaning individual consumers cannot be identified. **(For Now)**

47% Increase in Identity Theft in 2015

Cyber Security Facts

- **230,000** malware variants created everyday.
  (84 million created in 2015)
- Signature based technology used in AV software, IPS devices, and Web gateways is ineffective due to polymorphic malware changing constantly.
- Drive-by downloads have become the top web threat (Water Hole Attacks).
- Phishing is the number one attack vector.

FireEye

Recent Large Data Breaches

LastPass ****
The Last Password You'll Ever Need.

livingsocial

D&B

THE HOME DEPOT

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Domino's

]HackingTeam[

ups

BlueCross BlueShield

SONY

UBER

STAPLES

ARMY NATIONAL GUARD

IRS

JPMorgan

HARVARD UNIVERSITY

Data Breaches > 30,000 Records

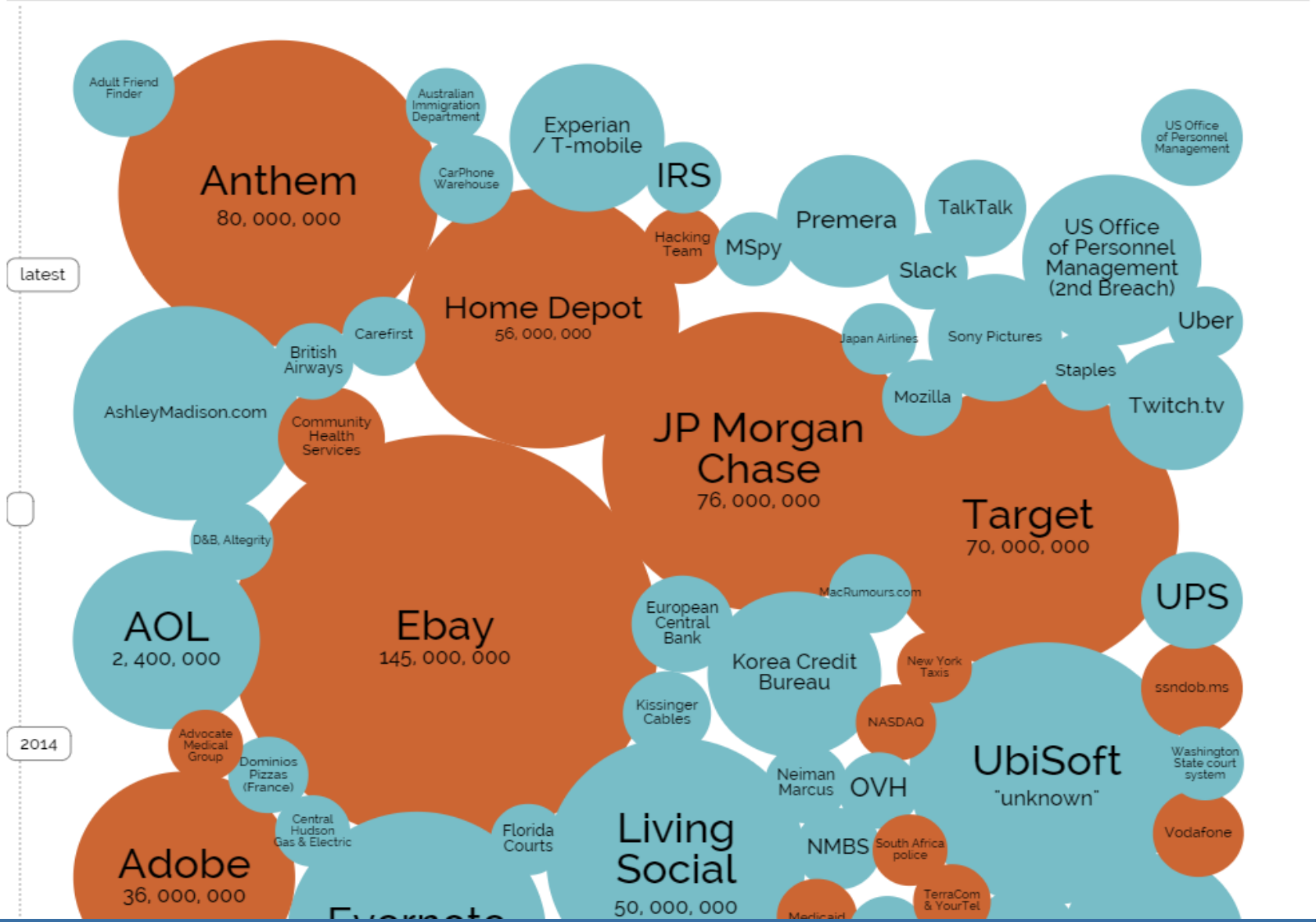
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 2nd October 2015)

interesting story

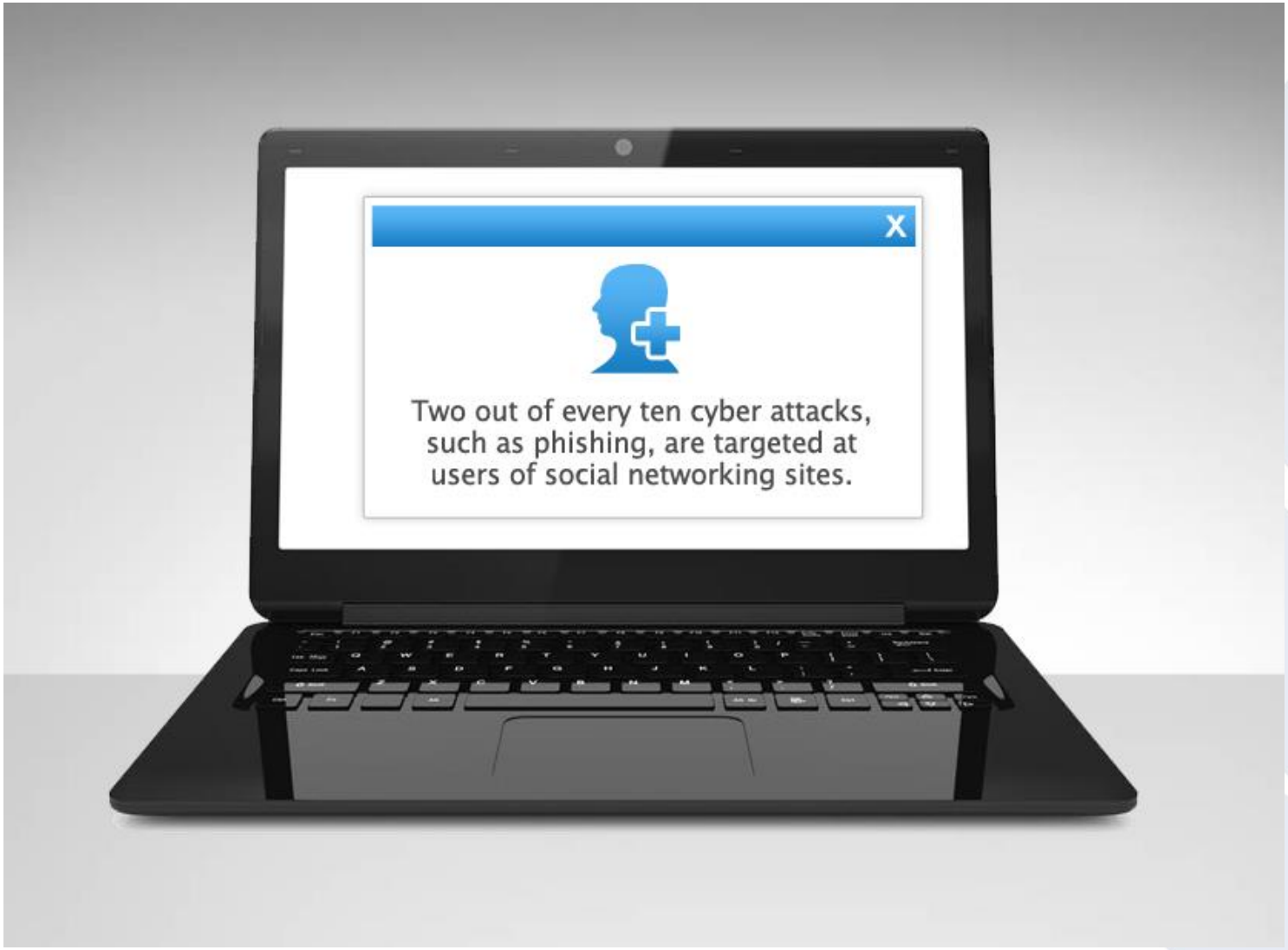
YEAR | BUBBLE COLOUR: YEAR | METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Privacy Facts - Malware

Privacy Facts – Social Media



Privacy Facts – ID Theft

TRUSTe PRIVACY INDEX

2014 CONSUMER CONFIDENCE EDITION

CONSUMER CONCERN

Consumer Concern
Consumer Concern remains high. 92% of US internet users worry about their privacy online compared with 89% in January 2013 and 90% in January 2012.

CONSUMER TRUST

Consumer Trust
Consumer trust continued to fall last year. 55% of US internet users trust businesses with their personal information online, compared with 57% in January 2013 and 59% in January 2012.

BUSINESS IMPACT

Business Impact
Business impact remains high. 89% of US internet users say they avoid companies that do not protect their privacy compared with 89% in January 2013 and 88% in January 2012.

Question: Do you have a right to be left alone?

What is Privacy?

- **Privacy has many meanings.** The most general is freedom from interference or intrusion, **the right "to be let alone“**

- American common law has recognized four types of actions for which one can be sued in civil court for invasion of privacy.
  1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
  2. Public disclosure of embarrassing private facts about the plaintiff.
  3. Publicity which places the plaintiff in a false light in the public eye.
  4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. (Identity Theft)

The Right of Privacy

- The word "privacy" is actually never used in the text of the United States Constitution. The Constitution, protects against state actors. Invasions of privacy by individuals can only be remedied under previous court decisions.
- The Fourth Amendment to the Constitution of the United States ensures that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".
- The First Amendment protects the right to free assembly, broadening privacy rights.
- The Ninth Amendment declares that the fact that a right is not explicitly mentioned in the Constitution does not mean that the government can infringe on that right.
- The Supreme Court recognized the Fourteenth Amendment as providing a substantive due process right to privacy. ".

WIKIPEDIA
The Free Encyclopedia

Only 3 States have “**privacy**" laws expressly stated in their State Constitutions.

- **California.** Article 1, §1 of the California Constitution articulates privacy as an inalienable right.

- **Florida.** Article I, §23 of the Florida Constitution states that "Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.“

- **Montana.** Article 2, §10 of the Montana Constitution states that "The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest".

States with Privacy Laws

WIKIPEDIA
The Free Encyclopedia

Right to be Forgotten European Union

- May 13, 2014 the European Court of Justice legally solidified that the "right to be forgotten" is a human right when they ruled against Google.

- Individuals "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."

WIKIPEDIA
The Free Encyclopedia

Right to be Forgotten European Union

- Concerns about its impact on the right to freedom of expression, censorship and a rewriting of history.

- The right to be forgotten is distinct from the right to privacy, due to the distinction that the **right to privacy constitutes information that is not publicly known**,

- Whereas the **right to be forgotten involves removing information that was publicly known at a certain time** and not allowing third parties to access the information.

WIKIPEDIA
The Free Encyclopedia

Fundamental Privacy Principles

- Don’t collect or retain more data than you reasonably need;
- Tell consumers how you plan to use and share their data;
- Give consumers choices about their privacy; and
- Protect data from unauthorized access.

Question: Should Privacy "desires" trump Legal Processes?

FBI vs. Apple

National Security

Privacy

The Public Relations War

Apple is being asked to provide "**reasonable assistance**" to the investigation of the San Bernardino attacks by disabling security preventing the FBI from accessing the encrypted handset of one of the shooters.

The PR War

Google chief executive Sundar Pichai. "Forcing companies to enable hacking could compromise users' privacy."

Jan Koum, the creator of Whatsapp, owned by Facebook, "We must not allow this dangerous precedent to be set. Today our freedom and our liberty is at stake."

The Information Technology Industry Council (lobbying group representing Google, Facebook, Microsoft, Samsung). "Our fight against terrorism is actually strengthened by the security tools and technologies created by the technology sector, so we must tread carefully given our shared goals of improving security, instead of creating insecurity."

Edward Snowden…FBI was "creating a world where citizens rely on Apple to defend their rights, rather than the other way around".

"will set a precedent and it will be the **end of life** on this planet"

"the software equivalent of cancer".

government is asking for the creation of software that doesn't exist, an abuse of the law and violation of the company's constitutional rights

"weakening encryption codes could have a "chilling effect" on First Amendment rights."

"…being forced to comply would set a dangerous precedent allowing broad access to law enforcement."

"Once the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound."

What is Apple specifically being asked to do?

- Apple can't break the encryption on the iPhone (or its other products). FBI has asked the company to disable certain features that would help its agents to unlock the iPhone.
- The FBI wants a special version of the iPhone's software that only works on the recovered device.
- Apple has to sign it with its secret keys in order to install it on the subject's iPhone.
- This custom version will "bypass or disable the auto-erase function" so it will not wipe the phone after a number of failed passcode guesses.

What is Apple specifically being asked to do?

- Apple must also modify the software on the subject's iPhone will not "purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware."
- Instead of forcing someone to type in passcodes manually, Apple must "enable the FBI to submit passcodes" to the subject's iPhone through an FBI device.
- The FBI will ship the iPhone to Apple, so that the company's proprietary code or secret keys never leaves the campus.

FBI vs. Apple - Arguments

- Apple - government has no legal right to compel it to assist in a government investigation, or to compel it to alter or destroy its business model of guaranteeing the safety and privacy of its customers' data.

- Any "key" it creates for the FBI is itself vulnerable to hacking, thereby jeopardizing all Apple products and negating the privacy of tens of millions, and even exposing the government to foreign hackers.

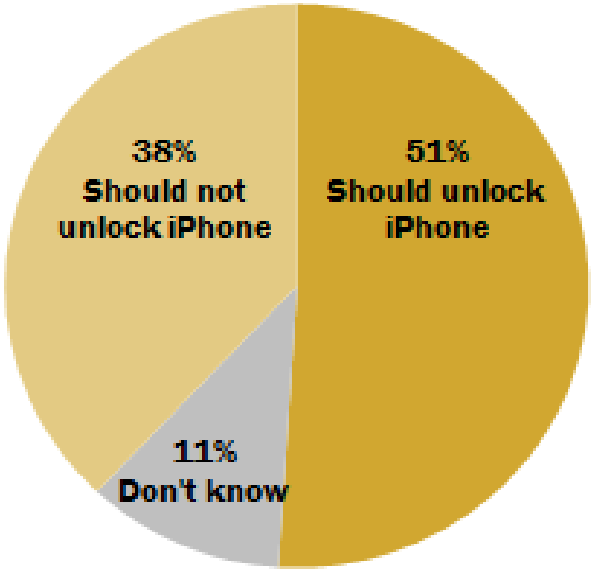
- Department of Justice - Apple has a legal duty to help solve the mystery of who knew about the San Bernardino attacks so that the guilty can be prosecuted and the rest of us protected from future harm. Government would keep secure whatever key Apple created.

FBI vs. Apple – Legal Points

- The latest national survey by Pew Research Center, conducted Feb. 18-21 among 1,002 adults, finds that almost identical shares of Republicans (56%) and Democrats (55%) say that Apple should unlock the San Bernardino suspect's iPhone to aid the FBI's ongoing investigation.

About half say Apple should unlock terror suspect's iPhone; 38% disagree

In response to court order tied to ongoing FBI investigation of San Bernardino attacks, Apple ...



Source: Survey conducted Feb. 18-21, 2016.
Figures may not add to 100% because of rounding.

PEW RESEARCH CENTER

“FBI is seeking 'dangerous power' that violates its constitutional rights”

- Federal judge overstepped her authority and violated the company’s constitutional rights.
- Order violates the 1st Amendment’s protections against forced speech — in this case, written computer code — and the 5th Amendment, which guards against government incursions on property and liberty.
- Prosecutors argued that the All Writs Act gives a judge the authority to compel Apple to write the new code. The act, which was first passed by Congress in 1789 and updated periodically, is a sweeping legal tool that allows judges to issue orders if other judicial avenues are unavailable.

Privacy or Marketing

- Apple had cooperated with the government by turning over all data pursuant to a valid search warrant.
- The information that was sought from Farook's iPhone had not been backed up, so the government could not conduct a simple search on its own to get it. Instead, it had to attack the encryption systems built into the phone itself.
- Farook did not own the phone; his employer did, and it gave consent to the search. This knocked out any Fourth Amendment claim that the government intended to perform some unreasonable search and seizure.

Privacy or Marketing

- Apple alleges FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority."
- All Writs Act - "All courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."
- There are thousands of government applications each year under the All Writs Act.
- Language is no more problematic than the text of the Fifth Amendment, which holds that the United States shall not deprive any person "of life, liberty or property, without due process of law."

How it will end???

- Although the Courts will decide the legal merits of this case, the underlying arguments on both sides will not be settled until Congress takes action with specific legislation balancing privacy issues, national security and new technology.

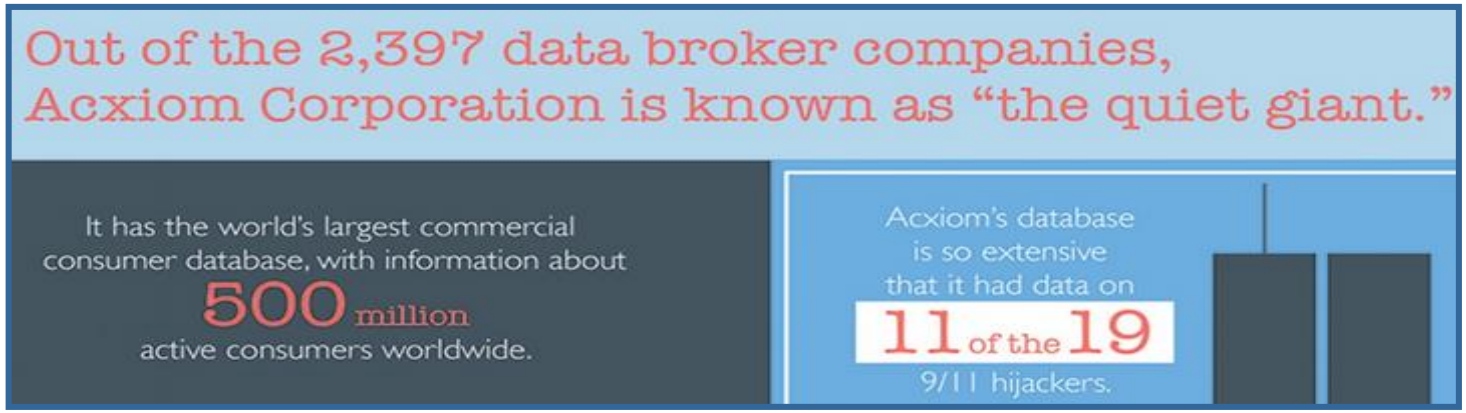
Question: Are you the Customer or the Product?

The Data Brokers

Who Owns Your Data?

The Data Brokers

- Companies that track our every move and then sell private details about our personalities to businesses
- According to the FTC, there are **no current federal laws requiring data brokers to maintain the privacy of consumer data** unless they use that data for credit, employment, insurance, housing, or other similar purposes.
- **$156 billion industry**
- The Senate commerce committee and the FTC have been investigating them



The Data Brokers

Where do they get this data?

There are three primary types of sources:

Acxiom 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.

Public

Government records, public records, publicly available data

Volunteered

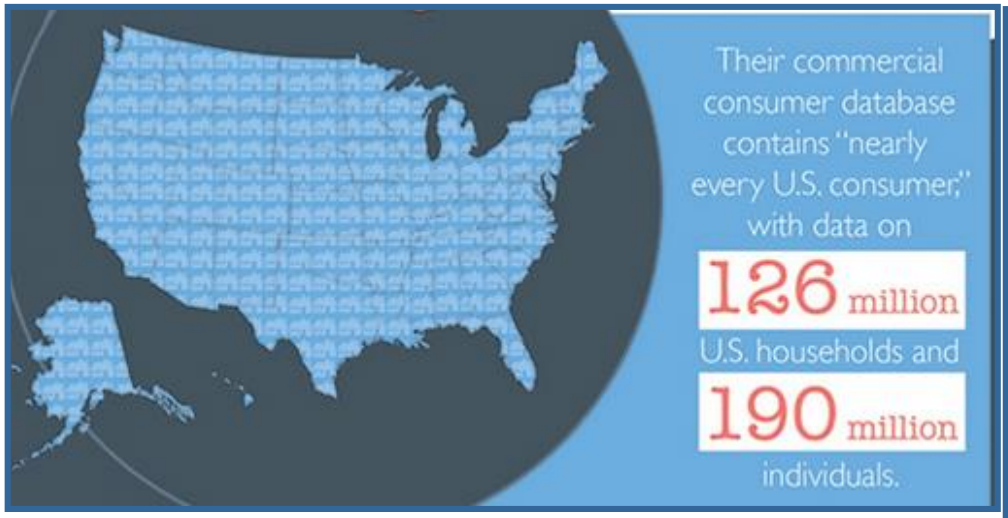
Self-reported data from surveys and questionnaires

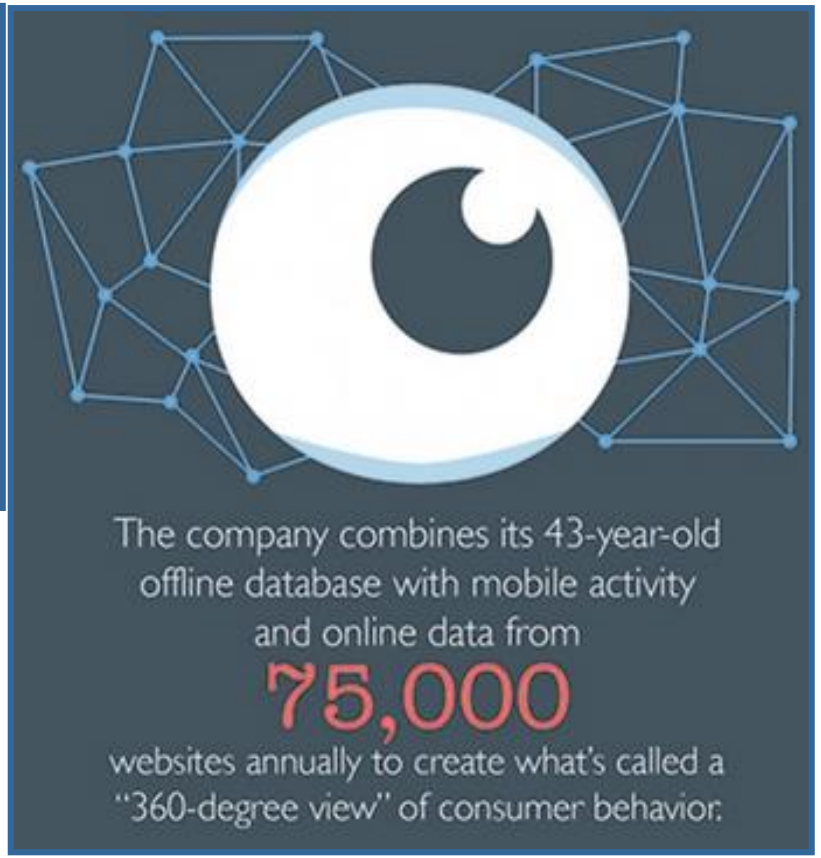
Private

Mostly data from other commercial entities, employers, online trackers

The Data Brokers

acxiom





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.

The Data Brokers

acxiom

Email

- Make a Purchase Via Internet
- Make a Purchase Via Phone
- Mobile Social Networker
- Use a Smart Phone
- Childrens Age Ranges Present in Household
- Home Owner / Renter
- Economic Stability Indicator
- Age in Two--Year Increments
- Gender
- NetWorth -- Gold

Mobile

- Make a Purchase Via Internet
- Make a Purchase Via Phone
- Childrens Age Ranges Present in Household
- Home Owner / Renter
- Use a Smart Phone
- Income Code -- Estimated Household
- NetWorth -- Gold
- Age in Two--Year Increments
- Gender
- Cord Cutter Propensity

Social

- Social Influencer
- Socially Influenced
- Mobile Social Networker
- Heavy Facebook User
- Heavy Twitter User
- Heavy LinkedIn User
- Heavy YouTube User
- Photo Poster
- Video Poster
- Business Fan

Automotive

- Presence of Children
- Income Code -- Estimated Household
- NetWorth -- Gold
- In Market for a New Domestic Luxury Vehicle
- In Market for a New Domestic Regular Vehicle
- In Market for a New Japanese Luxury Vehicle
- In Market for a New Japanese Regular Vehicle
- In Market for a New Korean
- Pay Cash for a New Vehicle
- Finance a New Vehicle

Financial Services

- Income Code -- Estimated Household
- Home Owner / Renter
- Economic Stability Indicator
- UnderBanked
- NetWorth -- Gold
- Heavy Transactors
- Shopped for Banking Services Via the Internet
- Full Service Investor
- Self--Service Investor
- Employment Status
- Have Online Trading Account

Insurance

- Presence of Children
- Income Code -- Estimated Household
- Home Owner / Renter
- Networth Gold
- You and Other Household Members Have Medical Insurance
- You Alone Have Medical Insurance
- Obtain Medical Insurance from an Agent Representing One Company
- Obtain Medical Insurance from Agent or Broker Representing Many Companies
- Obtain Medical Insurance Through the Internet
- Have Long Term Care Insurance

The Data Brokers

acxiom

Non-Profit

- Income Code -- Estimated Household
- NetWorth -- Gold
- Age in Two--Year Increments
- Childrens Age Ranges Present in Household
- Community Involvement -- Causes Supported Financially
- Green Living Lifestyle Propensity
- Written or Called any Politician at the State, Local, or National Level
- Member of Charitable Organizations
- Contribute to Public Broadcasting Service
- Engaged in Fund Raising Activities

Political

- Childrens Age Ranges Present in Household
- Home Owner / Renter
- Community Involvement -- Causes Supported Financially
- Green Living Lifestyle Propensity
- Written or Called any Politician at the State, Local, or National Level
- Congresssional District
- State legislature assignment for the upper level (senate)
- State legislature assignment for the lower level (house)
- Political Party
- Age in Two--Year Increments

Retail

- Childrens Age Ranges Present in Household
- Presence of Children
- Income Code -- Estimated Household
- Home Owner / Renter
- Networth Gold
- Technology Adoption
- Infobase--X Affordability
- Purchase Apparel from an Upscale Store
- Purchase Apparel from an Online Pure Play Store
- Purchase Apparel from a Mass Merchant

Telecom

- Childrens Age Ranges Present in Household
- Home Owner / Renter
- Economic Stability Indicator
- Income Code -- Estimated Household
- Purchase a Smartphone Mobile Phone
- Purchase Consumer Electronics from a Website Retailer Store
- Purchase Consumer Electronics from a Website Vendor Store
- Cricket/Leap/Jump Mobile Phone Customer
- Technology Adoption
- Cord Cutter Propensity

Travel & Entertainment

- Childrens Age Ranges Present in Household
- Presence of Children
- Income Code -- Estimated Household
- Networth Gold
- Shopped for Airline Tickets Via the Internet
- Travel -- Frequent Flyer
- Bought Travel Services Via the Internet
- Number of Hotel Room Nights Stayed for Either Leisure or Business in the Last 12 Months
- Take a Cruise
- Affinity for a Suite Room

Games

- Childrens Age Ranges Present in Household
- Presence of Children
- Income Code -- Estimated Household
- Gender
- Age in Two--Year Increments
- Games -- Video Games
- Product Propensities: Own a Wii
- Product Propensities: Own a Xbox
- Product Propensities: Own a PlayStation
- Technology Adoption

The Data Brokers

acxiom

Sample List of Targeting Products Identifying Financially Vulnerable Populations

APPENDIX II

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

What Marketers may know about your personal and public life

1. **They know how much you're worth.** Data brokers routinely collect information about your estimated income and what kind of job you have. They also mine information about how much your home is worth and whether you recently filed for bankruptcy or have a lien against your house. They might tag you and your spouse as "new money," "young and thrifty," "retirement ready," "prosperous parents," "social insecurity" or "jumbo mortgagees."

2. **They know what kind of car you drive.** Collect detailed information about the car you own due to public record searches.

3. **They know your hobbies and if you're good with money.** They have a list of what your hobbies are based on your purchasing history and can target you with advertisements for that hobby. Go beyond simple ad-matching and gauge what kind of shopper you are -- how likely you are to pay a certain price for a particular item.

What Marketers may know about your personal and public life

4. **They know about your health worries.** Pharmacies may legally sell your prescription information to third parties, as long as your name isn't tied to the data. Marketers also have access to any information you "voluntarily" self-report through consumer surveys, sweepstakes prizes, warranty card registrations, certain types of telephone and rebate coupons and registrations at relevant trade shows.

5. **They know what you did last summer.** Based on your purchasing data brokers know what you do with your time off work. Regularly collect information about any public licenses you hold (ie. hunting, fishing, boating, etc.)

6. **They know about your love life.** May have access to intimate details about your life. 2012 Wall Street Journal investigation of dating site OKCupid, has previously shared information with third parties about users' self-reported sexual orientation, as well as their drug use and smoking habits.

What Marketers may know about your personal and public life

7. **They know how much time you spend on Facebook.** Marketers track the pages you visit, the time you spend on each site and whether you bought anything. Look at which search terms you use, record your social media activity, and follow you around as you browse different sites. Capture public tweets, Facebook likes, comments or reviews you make available online.

8. **They know where you hang out.** If you have an app that uses location-based services, the app can track your movements and follow you around town. May be able to track you using the Wi-Fi on your device.

9. **They know your race, ethnicity and religious affiliation.** Collect a variety of demographic information about who you are and what kind of environment you live in. May sell information about how many kids you have, whether you're married or single and how many people live in your house.

What Marketers may know about your personal and public life

10. **They know what you like to read, listen to and watch.** Magazine publishers regularly trade your subscription information so other publishers can target you with offers for similar publications. Music streaming services, meanwhile, may share "anonymized" information about your listening history (or information you make public). Video streaming services, such as Hulu, now have the legal ability to share what you watch with third parties, as long as they ask for your permission first.

11. **They know if you just got married or had a baby.** Targeting you with offers timed to special events “life event triggers” -- buying a house, getting married or moving to a new home.

12. **They know which political party you support.** May also be able to guess your political leanings, based on publicly available information, such as your voting records and campaign contributions.

What you can do if you don't want to be followed?

1. **Delete Cookies.** Cookies let websites collect information about what else you do online. Most browsers have privacy settings that let you block third-party cookies.

2. **Log Out of Social Media Sites While You Browse the Web.** Use different browsers for different online services -- don’t go to a shopping site while you are logged in to Facebook.

3. **Change Your Smartphone’s Privacy Settings.** You can change the privacy settings on your iPhone or Android device to limit ad tracking.

4. **Skip Store Loyalty Cards.** Data brokers collect information from the real world too, Hans says. If privacy is really important to you, decline offers for store loyalty cards–a major way retailers gather information about your buying habits. The downside? You may miss out on discounts.

What you can do if you don't want to be followed? (cont)

5. **Employ Advanced Online Tools.** Disconnect.me can help you see and block tracking requests as you spend time online. Instead of Google, you can try the DuckDuckGo search engine, which promises not to collect or share personal information. Or use the browser Tor, which lets you go online anonymously.

6. **Opt-out of Data Broker Collection—Whenever Possible.** Ultimately, it's difficult to get data brokers to stop collecting information about you, or even find out how much information brokers already have. The FTC concluded that to date, "consumer opt-out requests may not be completely effective."

7. **Do a Digital Check-up**. Many popular sites like Facebook, Amazon, and Twitter offer privacy controls, so use them. Every once in a while, check your settings and see if you're happy with how you are limiting the ways your data is used.

Epsilon Data Breach

April 4, 2011

- Epsilon is the world's largest provider of email marketing.
- Epsilon fell to a spear-phishing attack in 2011.
- Conservative estimates are that 60 million customer emails addresses were breached.
- Epsilon sends more than 40 billion emails a year on behalf of 2,500 brands. The breach affected Kroger, TiVo, Marriott Rewards, Ritz-Carlton Rewards, US Bank, JPMorgan Chase, Capital One, Citi, McKinsey & Company, New York & Company, Brookstone, BestBuy, and Walgreens.

Payment of over $225 million in damages reported

Who's Tracking You?
Tracking Cookies

- Data that is distributed and shared across two or more unrelated Web sites for the purpose of gathering information to present customized data to you.
- Not harmful like malware, worms, or viruses, but can be a privacy concern.
- Advertising company can determine all the sites you have been to if they have cookies present on those sites.

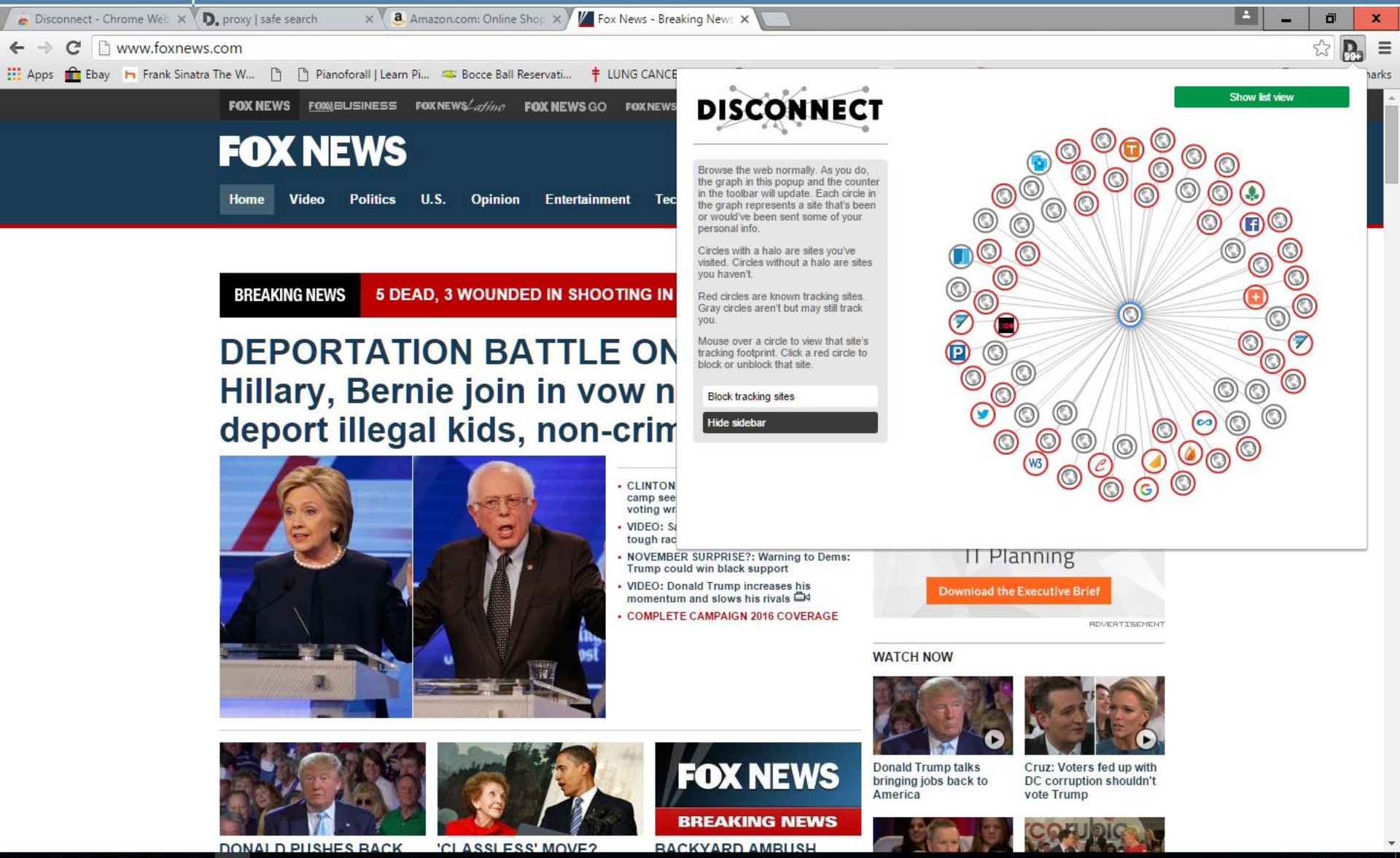
Who's Tracking You?
Flash cookies: a cause for concern?

- Because browser-based cookies are easy to detect and delete, some advertisers are now using "flash-based" **supercookies** which are not stored on your computer like browser-based cookies.
- Result, they are **harder to find and delete**.
- Acts as a second level of authentication in addition to the user's login and password.

Who's Tracking You?
Social networking tracking

- Most social networking tracking occurs through Javascript social buttons like "Like" and "Tweet" buttons.
- Connections are made to entirely different companies than the website you're actually visiting.
- More than a quarter–26.3%– of what your browser does when you load a website is respond to requests for your personal information, leaving the remaining 73.7% for things you want your browser doing, like loading videos, articles, and photos.

Web Tracking



Who's Tracking You?
Web beacon -- a 1-pixel image

- Web beacons are tiny image files invisible to users and are used to transmits information to advertisers. Commonly used in emails.
- WSJ examined 1,000 top websites and found that approximately 75 percent of them featured social networking code that can match users' online identities with their web-browsing activities.
- Nearly 25% of the web's 70 most popular sites shared personal data, like name and email address, with third-party companies.

Verizon fined $1.35 million by the FCC for using "supercookies (March 7, 2016)

- Fined $1.35 million by the FCC for sending undeletable special data headers, or "supercookies" to more than 100 million customers from 2012 until 2014.
- The unique identifier headers (UIDHs), or supercookies, were inserted into the mobile Internet traffic of Verizon customers without their knowledge or consent to deliver targeted ads from Verizon and third parties.
- Verizon has agreed to notify consumers about its targeted advertising programs and will obtain opt-in consent from its customers before sharing UIDHs with third parties or within Verizon.

What Information Does Your Service Provider Collect and Store?

Service providers (like AT&T, Sprint, Verizon, and T-Mobile) collect the following:

- Incoming and outgoing calls: the phone numbers you call, the numbers that you receive calls from, and the duration of the call;
- Incoming and outgoing text messages: the phone numbers you send texts to and receive texts from;
- How often you check your e-mail or access the Internet;
- Your location.

Unfortunately, there is nothing you can do about your service provider collects.

Sprint verizon at&t

Question 4: What can/should you do?

Business Privacy Responsibilities

1. **Know the Law**
2. **Protect Customer Information**
3. **Protect Employee Information**

Privacy Law

- **The Electronic Communications Privacy Act (ECPA) 1986.** Can apply to both law enforcement agencies and companies. ECPA makes it unlawful under certain circumstances for someone to read or disclose the contents of an electronic communication.
- **The Computer Fraud and Abuse Act.** The 1984 Computer Fraud and Abuse Act was enacted to prevent unauthorized access to computers. Used in prosecuting hackers, and covers information stored on computers.
- **Children's Online Privacy Protection Act (COPPA).** The 1998 COPPA protects the privacy of children under the age of 13 by prohibiting the online collection of a child's personal information without providing notice and obtaining parental consent. Prohibits requiring that a child disclose more information than is reasonably necessary to participate in an activity online.
- **The Federal Trade Commission.** Investigates and brings an enforcement action against an entity it believes is engaging in an unfair or deceptive act or practice.

Cybersecurity Information Sharing Act of 2015 (CISA)

- The Cybersecurity Information Sharing Act protects the liability of private sector entities when sharing and receiving cyber threat information.

- It also establishes the personal data that needs to be removed before data sharing can occur and how quickly individuals must be notified their information was shared.

Protecting Customer Information
Your Web Site's Privacy Statement

1. **Review your privacy statement to make sure it's easy to read and understand.**

   Build trust with your consumers: write your privacy statement in straightforward language and organize it clearly.

2. **Make sure your privacy statement aligns with your terms-of-service statement.**

   Confirming uniform privacy practices throughout your Website projects a clear and concise impression to consumers while minimizing your exposure to privacy risk.

3. **When establishing your company's privacy program, build internal documents with an eye to your public privacy statement.**

   Make sure that your internal documents and policies reflect your outward-facing privacy

Protecting Customer Information
Your Web Site's Privacy Statement

4. **Review your privacy policy regularly to make sure it accurately reflects your current data-collection and -handling practices.**

   Establish annual business privacy review process; should involve all parties who handle customer data–at minimum, management, marketing, legal, operations, and IT.

5. **When writing or revising your privacy statement, use may or might statements sparingly.**

   Avoid sounding evasive and build trust upfront by using forthright language.

6. **Add an effective date to your privacy statements.**

   The statement can be as simple as "Effective as of January 1, 2004."

Protecting Customer Information
Your Web Site's Privacy Statement

7. **Minimize data collection on your Website.**

   Only collect enough personal data from visitors to either provide them with your products or services or let them interact on your site.

8. **When you collect consumer data on your site, take extra steps to inform users about how their information will be used.**

   Communicate your practices to consumers transparently. Most organizations do this by providing a link to their privacy statement on the site's homepage or on pages that ask for personal information.

9. **Retain customer data for the shortest time possible.**

   Retain data for only as long as it serves a business purpose or as required by law.

SmartPhone Tips

1. **Password protect it.** 7 million smartphones lost/stolen each year.

2. **Shop online only** with **reputable** shopping app.

3. **Always close out of sensitive apps** (banking, finance, etc.) when finished.

4. **Do not automatically connect to any available WiFi connections.**

5. **Disable Bluetooth when not actively using it.** Hackers can steal personal information using Bluetooth when relatively close to you (less than 30 feet away); can occur undetected in an airport, hotel lobby, restaurant, or conference.

SmartPhone Tips (cont.)

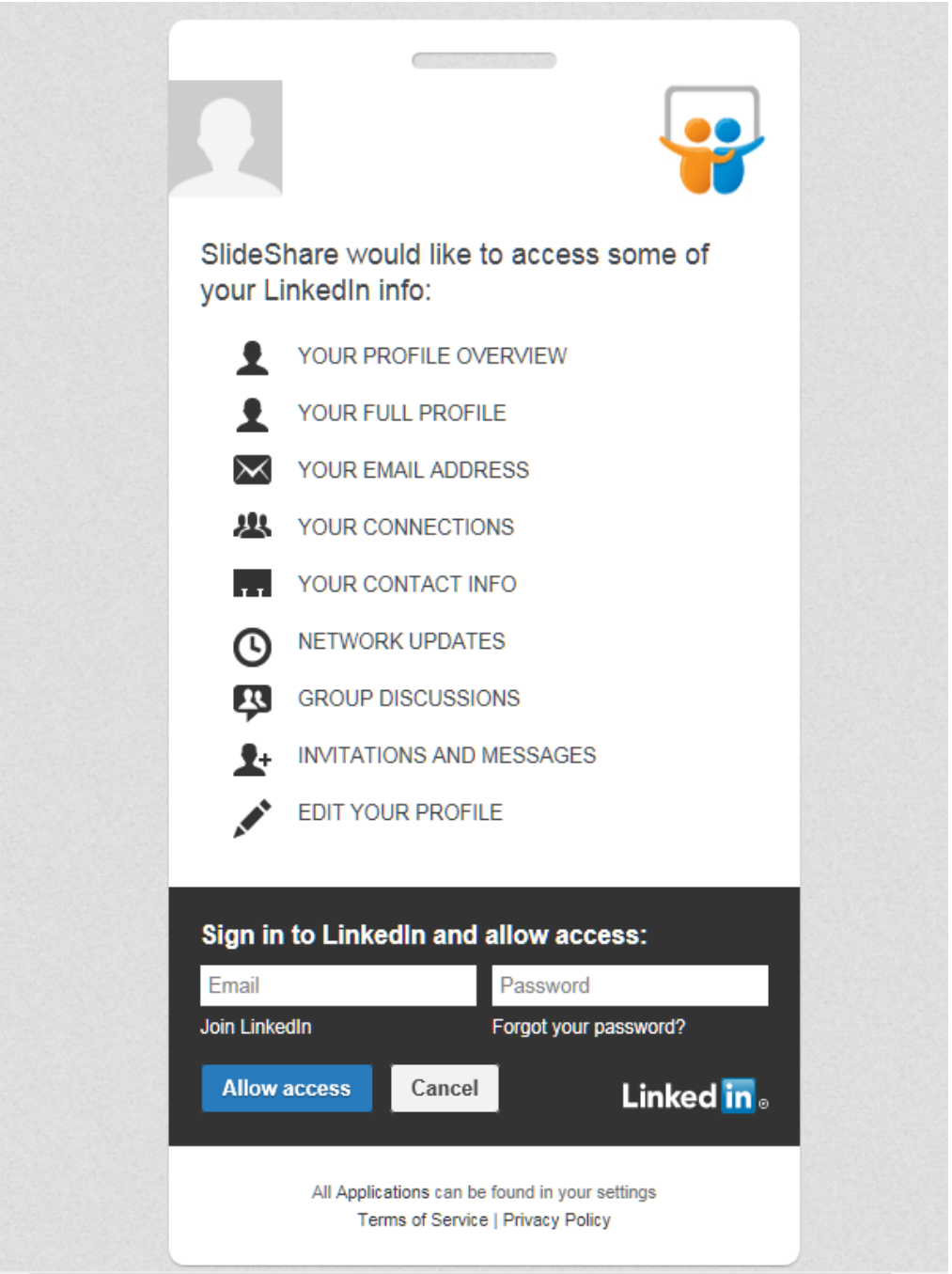
6. **Purge/wipe data from old smartphones** when donating/selling device.

7. **Beware of "free" Apps.** Downloading one gives the app complete access to your phone, which a fraudster can use to steal your credit card and bank account info.

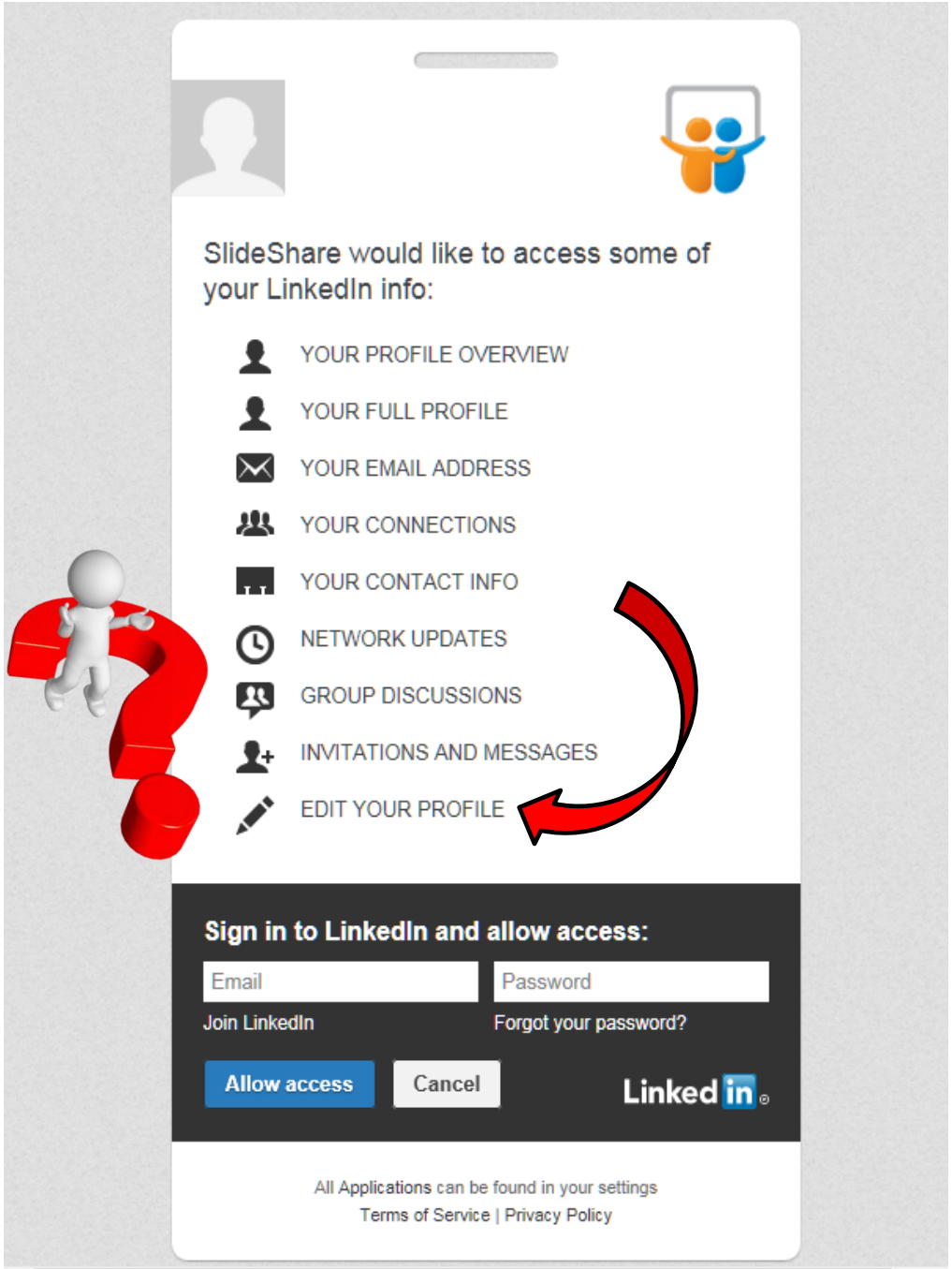
8. Do not store sensitive data on smartphone.

9. **Clear browser history.** By retracing your steps, a phone thief can use your history to hijack your accounts, steal your money and wreck havoc.

10. **Install remote wiping software.** Your identity is your asset. It is up to you to vigorously defend and protect it.



- Websites and apps are asking for greater access to your personal information.
- Are you reading what you are authorizing before allowing access?



- Websites and apps are asking for greater access to your personal information.
- Are you reading what you are authorizing before allowing access?

Questions & Answers

Backup Slides

Steps you can take to limit your exposure

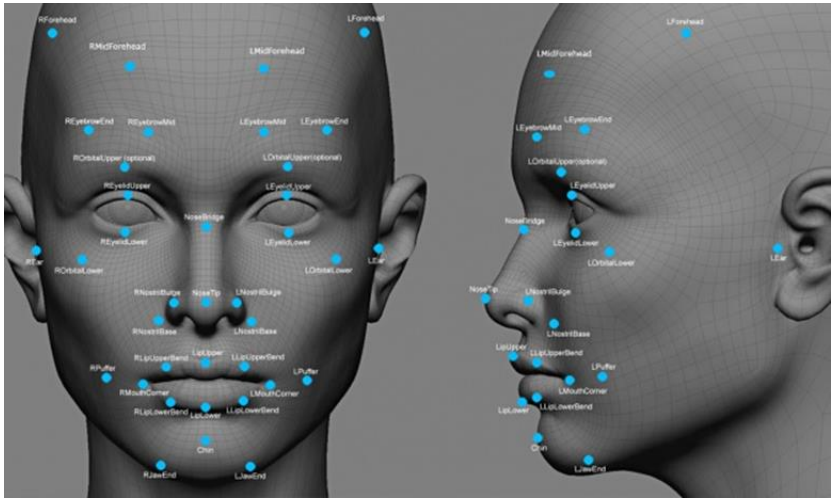
- Be careful about sharing your email address as well, since that information can also be used to connect you with other data.

- Most data brokers will also allow you to opt out of their data collection programs. However, you'll have to research each one individually and follow the directions on their websites.

- If you're tired of targeted ads online, look for a little blue triangle turned on its side next to any ad. If "you click on that icon, it will take you immediately to a place where you're told about what interest-based ads are and link to a place where you can opt out.“

- **http://www.stopdatamining.me/**

Facial recognition: is the technology taking away your identity?



- Facebook has created a tool, "DeepFace“, almost as accurate as the human brain when it comes to saying whether two photographs show the same person – regardless of changes in lighting and camera angles. A human being will get the answer correct 97.53% of the time; Facebook's new technology scores an impressive 97.25%.

- Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere – on a lamp post, attached to an unmanned aerial vehicle or, now, integrated into the eyewear of a stranger.

IRS Data Breach – May 2015

- **724,000 US tax payers** were affected by an IRS data breach in May 2015.
- Hackers used breached data to answer security questions used by the online service that enables US taxpayers to get copies of past tax returns.
- More than $5.8 billion in fraudulent refunds were made in 2013.
- IRS officials said that credit protection would be offered to taxpayers whose accounts were exposed.
- The IRS has urged US tax payers to file their tax returns as soon as possible to reduce the possibility of fraudsters doing so first.