# Privacy and Security

TEAM 1

# What Is Privacy?

- Freedom from observation, intrusion, or attention of others
- Society's needs sometimes trump individual privacy
- Privacy rights are not absolute
- Balance needed
  - Individual rights
  - Society's need
- Privacy and "due process"

# Need for Privacy

- Our lack of privacy leads to abuses, crime, and real negative societal consequences.
- Within little over one year there were 237 reported security breaches…
- Fundamental to a democratic society.
- Data is a corporate asset, like any other
- Assures our right to free speech, free assembly and a free press.

# Common Misperceptions

- *“I have anti-virus software…”*
- *“I don't personally have anything of value on my computer…”*
- *“I have a firewall…”*
- *“There are no major financial risks…”*

# Changing Nature of Threats

- Early threats were targeted on servers and computers connected to network to destroy them or use them to launch subsequent attacks
- Now threats are no longer operating systems, networks, or control of machines but rather…
- Personal data about the users on these machines for profit

*"Attackers are increasingly seeking financial gain rather than mere notoriety. During the past year we have seen a significant decrease in the number of large scale global virus outbreaks and, instead, are observing that attackers are moving towards smaller, more focused attacks"*

*Vincent Weafer – Senior Director at Symantec Corporation*

# What's the Potential Harm?

- Breaches of data privacy, data security can result in
  - Damage to reputation
  - Disruption of operations
  - Legal liability under new and amended laws, regulations, and guidelines, as well as under contracts
  - Financial costs

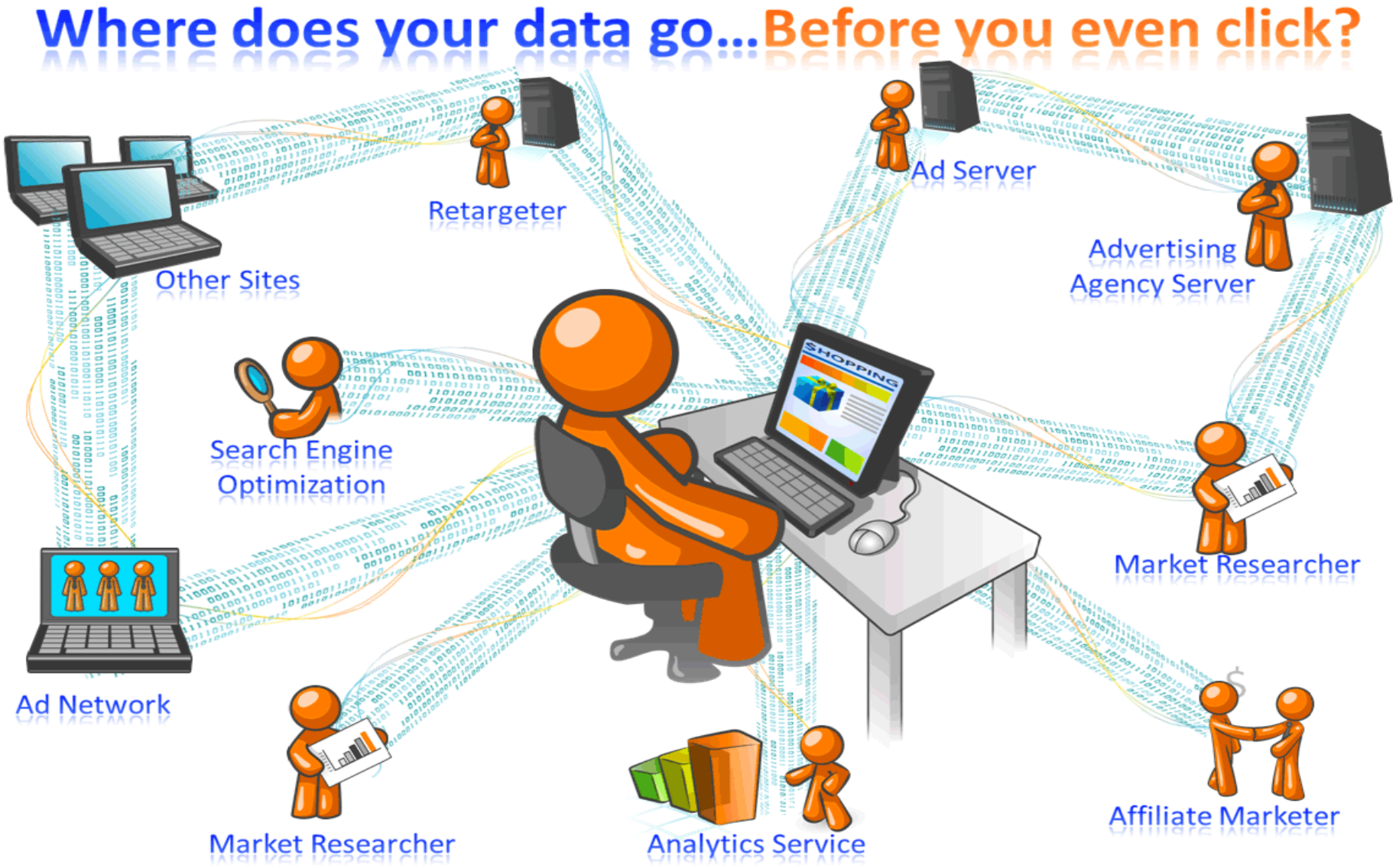
# Where should I worry about  privacy?

- Web Surfing
- Instant Messaging
- Chat Room/IRC
- P2P Networking
- Social Networking
- Online
- Banking/Finance
- Freeware/Shareware
- Search Engine
- VoIP
- Gaming
- Blogging
- Wiki's
- Everywhere

# Types of privacy threats

- Fraud
- Identity Theft
- Financial Loss
- Implication in
- Criminal Activity
- Cyber Stalking
- Cyber bullying
- Denial of health care
- Work place discrimination
- Denial of employment

# Shine a Light on Who's Watching You



# Criminals

- Criminals misuse many of these same technologies and business practices to violate your privacy.

- These have the financial means, expertise and are motivated by the same profit motives (however illegitimate.)

- Criminal data breaches are a major problem.

  Ex. Data breach data ends up on a underground market that is then used to personalize “email market” or phishing campaigns.

# Commercial

- Commercial - Search engines, websites, “free” email/IM, social networking sites.
- Mining this data is a multi-billion dollar industry that brings you online and off line advertisements
- Online marketing represents a revolution in marketing that allows untold understanding of your demographic & psychographic profile.
- Companies that don't properly invest in security technologies or their proper implementation are not protecting your privacy.

# Government

- Government is deeply involved in monitoring, analysis and mining of our internet/electronic activities.
- Sometimes beyond what most legal scholars would consider fair, objective, or even constitutional.
- Most legal scholars, technologists, citizens think we need big changes.
- Studies consistently show most American's want more privacy, checks and balances and due process.

# Government

- Government is doing the best job it can and many of them care very deeply about our privacy.
- All it takes is a few to abuse a system without checks and balances. .

- NSA Traffic Interception at AT&T
- FISA vs. US Constitution
- USA Patriot Act - Concerns
- Domestic Surveillance Debate

# What do they do with that data?

# Data Mining

- Data mining is correlating data from multiple sources to arrive at an understanding or result.
- In the marketing world it allow firms to have a deep understanding of your demographic and psychographic profile.
- As a result they sell to you better.
- Or annoy you more... =P

# Your personal data isn't yours

- Nearly all commercial entities that have your personally identifiable information (PII) claim ownership of your personal information.
- They utilize it, sell it to partners, share it with other organizations.  Your information is a valuable and lucrative commodity.
- Marketing, Direct Marketing, Online Marketing, Telemarketing

# What Should we try to protect?

**PII - Personally Identifiable Information**

- - Unique personal information used to identify you.
  - Full Name
  - Mother's maiden name
  - Banking information
  - Social security number
  - Credit card information
  - Address
  - Phone number
  - Password
  - Email addresses
  - Drivers License
  - Vehicle registration plate number

# Data breaches and Privacy

- Data breaches or computer security breaches expand the threat to privacy.
- Data then ends up in the hands of the cyber-criminals who use it for nefarious ends.
- They sell this data in the criminal underground.
- Ex. Carding networks sell stolen credit card info.

# Data Breaches since 2000

Also see: Privacyrights.org Chronology of Data Breaches

# Technological Solutions

- Perimeter and Interior Firewalls
- Virtual Private Network
- Intrusion Detection and Prevention System
- Enterprise Directory
- Filtering Technology
- Network Behavior Analysis

# Privacy and the Law

- No constitutional right to privacy
  - The word “privacy” is not in the Constitution
  - Congress has passed numerous laws
    - Not particularly effective
    - Issue is pace of change
- Privacy is a function of culture
- Privacy means different things in different countries and regions
  - Serious problem on global Internet

# Some Privacy laws.

| Year | Title | Intent |
|---|---|---|
| 1970 | Fair Credit Reporting Act | Limits the distribution of credit reports to those who need to know. |
| 1974 | Privacy Act | Establishes the right to be informed about personal information on government databases. |
| 1978 | Right to Financial Privacy Act | Prohibits the federal government from examining personal financial accounts without due cause. |
| 1986 | Electronic Communications Privacy Act | Prohibits the federal government from monitoring personal e-mail without a subpoena. |
| 1988 | Video Privacy Protection Act | Prohibits disclosing video rental records without customer consent or a court order. |
| 2001 | Patriot Act | Streamlines federal surveillance guidelines to simplify tracking possible terrorists. |

# What can I do to protect my privacy?

- Consider your interactions with the internet to be 100% public.
- Keep your computer up to date/patched.
- Keep an updated anti-malware suite.
- Don't download freeware or shareware unless you have validated it is spyware, adware, greyware free.
- Buy the official release.
- Read the EULA (End User License Agreement) and Privacy Policy.

# What can I do to protect my privacy?

- Read the privacy and terms of use policies of the firms you work with.
- Use a throw away email account with a pseudonym for non-critical communications.
- Give minimal information about yourself when its not required.
- Understand the legal rights firms have to demand certain PII information.
- Ex. If there is no state or federal law a firm shouldn't need your Social Security Number.
- Support organizations that fight for privacy rights such as EPIC, EFF, CDT.

# Web technologies That effect privacy

# Cookies

- Tracking cookies are morsels of plain text sent back and forth between a server and your browser.
- Used in authenticating and tracking you as a website user and hold preferences and details and required for some functionality.
- First Party (Site you are visiting) vs. Third Party (Ad Networks)
- You can control the settings in browser settings.

# Web Surfing

- Remember you have little privacy while surfing the web.
- Your ISP has full transparent view of your activities
- So do the websites, email services, search engines, instant messaging services, social networking sites.
- The sites that offer "free" services charge you with your PII (Personally Identifiable Information) and your privacy.

# Web Surfing

- If the information is not legally required i.e. its not a financial/government transaction then you don't need to provide it.
  Check state and federal law..
- Consider using an anonymizing proxy service such as Anonymizer.com,
  Hushmail Stealth Surfer, Tor or Jap.
- Optimally use Mozilla Firefox with AdblockPlus and NoScript to block all executable content unless explicitly allowed.

# IM/Chat

- No privacy of these communications.
- Privacy of your messages is not assured.
- 3rd parties can eavesdrop.
- Free service can further mine these for building a consumer profile on you.
- Many do support encryption (Yahoo, MSN).
- Encrypted Instant Messenger Clients - Wikipedia

# Social Networking

- Just as search engines, "free" email accounts and other websites mine your data so do Social Networking sites.
- More worrisome is that they create a climate in which people are willing to share details voluntarily they might not otherwise.
- They keep rich PII details.
- Be weary of the add on applications from social networking sites such as toolbars, IM clients.

# Social Networking

- Generally publicly available.
- Minimize PII.
- Don't use IM, Email or chat features if you are concerned with your privacy. No encryption and potentially infinite retention.
- Minimize posted to generally publically known information.

# Shareware/Freeware

- Can contain malware that might violate your privacy rights.
- If you really need the program, buy it.
- If you want a truly free program that has none of these problems - then get Free Software or Open Source Software.
- Read the fine print, EULA (End User License Agreement), Privacy Policy.
- If the vendor doesn't support the privacy you expect; go elsewhere.

# Phishing

- SPAM brings you messages that seem to be from legitimate parties that send you to phony/look-alike website.
- Your (Personally Identifiable Information) and credit card information is collected and sold in the underground.
- Usually an attempt is also made to infect your machine with malware.
- Best to not even open. Delete.

# Phishing Email Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Account cancel!
- Social Engineering – Attempt to mislead, persuade, confuse, etc.
- Generic or Targeted Greetings – Hello Distinguished Sirs!?
- Urgent Request for PII – We need to validate your account or you will be terminated from the internet!
- Forged Email. – Email is often not valid and or not from the domain in question.
- Incorrect Link – Link is obviously wrong. https://www.payppal.net/~noway

# What are Internet Cookies?

- A cookie is a type of message that is given to a browser by a Web server
- A cookie is information stored on your computer by a website you visit
- Cookies store your settings for a website, such as preferred language or location
- This allows the site to present you with information you needs

# Can Cookies be malicious?

- Cookies that watch your online activity are called malicious or tracking cookies
- These types of cookies can be used to store and track your activity online
- Many antivirus  today will flag suspicious cookies when scanning your system for viruses

# Surveillance and Monitoring

- Surveillance
  - Continual observation
  - Tampa – facial scanning at Super Bowl
  - Packet sniffing
- Monitoring
  - The act of watching someone or something
  - E-mail Web bugs
  - Workplace monitoring is legal

# Surveillance and Monitoring Tools

- Spyware
  - Sends collected data over back channel
- Snoopware
  - Records target's online activities
  - Retrieved later
- Screen shots, logs, keystrokes
- Other surveillance/monitoring sources
  - OnStar and GPS tracking
  - E-ZPass systems
  - Phone calls and credit card purchases

# What we need moving forward

- Be involved.
- Choose to support companies that reflect your privacy/security needs.
- Vote with privacy, security in mind for digitally literate politicians. The internet is NOT a series of tubes!
- Comprehensive laws protecting privacy which is flexible enough to adapt to new technology.

# What we need moving forward

- Laws like Europe Union.
- http://www.msnbc.msn.com/id/15221111/
- We should control our PII.
- We own our PII.
- We end up paying economic the social costs we shouldn't.

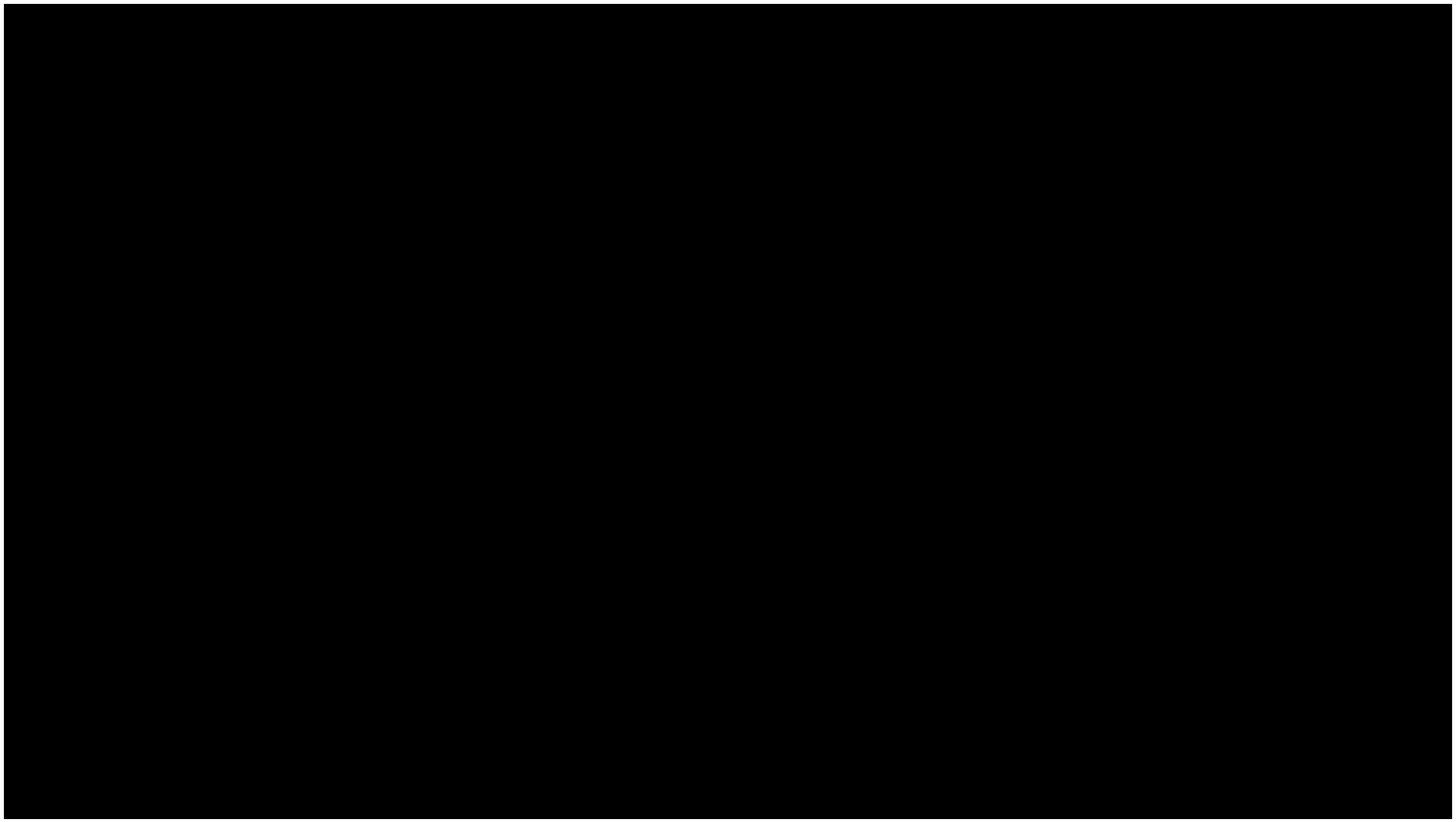
# Opt out

- National Do-Not-Call List
- Mass Do Not Call List
- Opt-out Preapproved Credit Cards -
- FTC - Legitimate Free Annual Credit Report

# Future Privacy Threats

- Genetic Testing
- RFID's
- Biometrics
- Real ID
- ISP monitoring and data mining
- GPS enabled cells

# Privacy Awareness Video 2013



# Conclusion

- Privacy and security are critical issues you can do something about.
- Its not all about technology. Its our choices and activities, laws/regulation, our political involvement **and** the technology .
- We can create a better world.