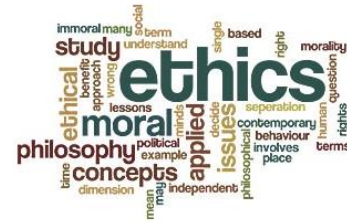


Introduction to MIS

IT Ethical and Legal
Issues

Learning Objectives



- Discuss information privacy and methods for improving the privacy of information
- Explain the privacy of e-mail, data collection issues, and censorship
- Discuss the ethical issues related to information technology
- Discuss the principles of intellectual property and issues related to the infringement of intellectual property
- Discuss information system issues that affect organizations, including the digital divide, electronic publishing, telecomputing, and the connection between the workplace and employees' health
- Describe green computing and the ways it can improve the quality of the environment

Ethics from Wikipedia

- **Ethics** (from the Ancient Greek "*ethikos*", meaning "arising from habit") is one of the major branches of philosophy, one that covers the analysis and employment of concepts such as right, wrong, good, evil, and responsibility
 - It is divided into three primary areas: *meta-ethics* (the study of what ethicality is), *normative ethics* (the study of what ethical truths there are and how they are known), and *applied ethics* (the study of the use of ethical knowledge)

■ Are ethical standards universal ?





Ethical Issues

- **Ethics.** A branch of philosophy that deals with **what is considered to be right and wrong within a particular context**



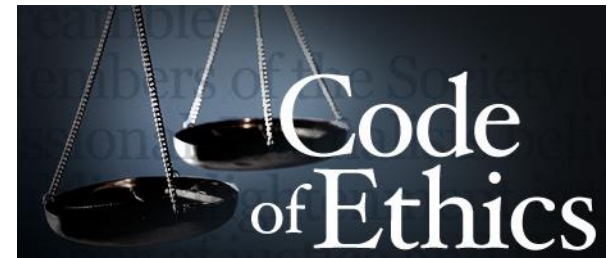
■ What do these organizations have in common?

- [Amazon](#)
- [Apple](#)
- [Dell](#)
- [Facebook](#)
- [Google](#)
- [Intel](#)
- [LinkedIn](#)
- [Microsoft](#)
- [Twitter](#)
- [Yahoo](#)





- A **Code of Ethics** is a collection of principles that are intended to guide decision making by members of an organization
- Why do most corporations and professional organizations have a code of ethics ?





Code of Ethics



- Corporations, professional organizations, trade associations, etc.

- [ServiceMaster Code of Ethics](#)

- Why have one ?

- to define acceptable behaviors (within the organization)
 - to promote high business and individuals standards
 - to provide a benchmark for people to use for self evaluation
 - to establish a framework for professional responsibility
 - as a mark of organizational maturity



Johnson & Johnson



Johnson & Johnson

PHARMACEUTICAL RESEARCH
& DEVELOPMENT, L.L.C.

We believe our first responsibility is to the doctors, nurses and patients,
to mothers and fathers and all others who use our products and services.
In meeting their needs everything we do must be of high quality.

We must constantly strive to reduce our costs
in order to maintain reasonable prices.
Customers' orders must be serviced promptly and accurately.
Our suppliers and distributors must have an opportunity
to make a fair profit.

We are responsible to our employees,
the men and women who work with us throughout the world.
Everyone must be considered as an individual.
We must respect their dignity and recognize their merit.
They must have a sense of security in their jobs.
Compensation must be fair and adequate,
and working conditions clean, orderly and safe.
We must be mindful of ways to help our employees fulfill
their family responsibilities.
Employees must feel free to make suggestions and complaints.
There must be equal opportunity for employment, development
and advancement for those qualified.
We must provide competent management,
and their actions must be just and ethical.

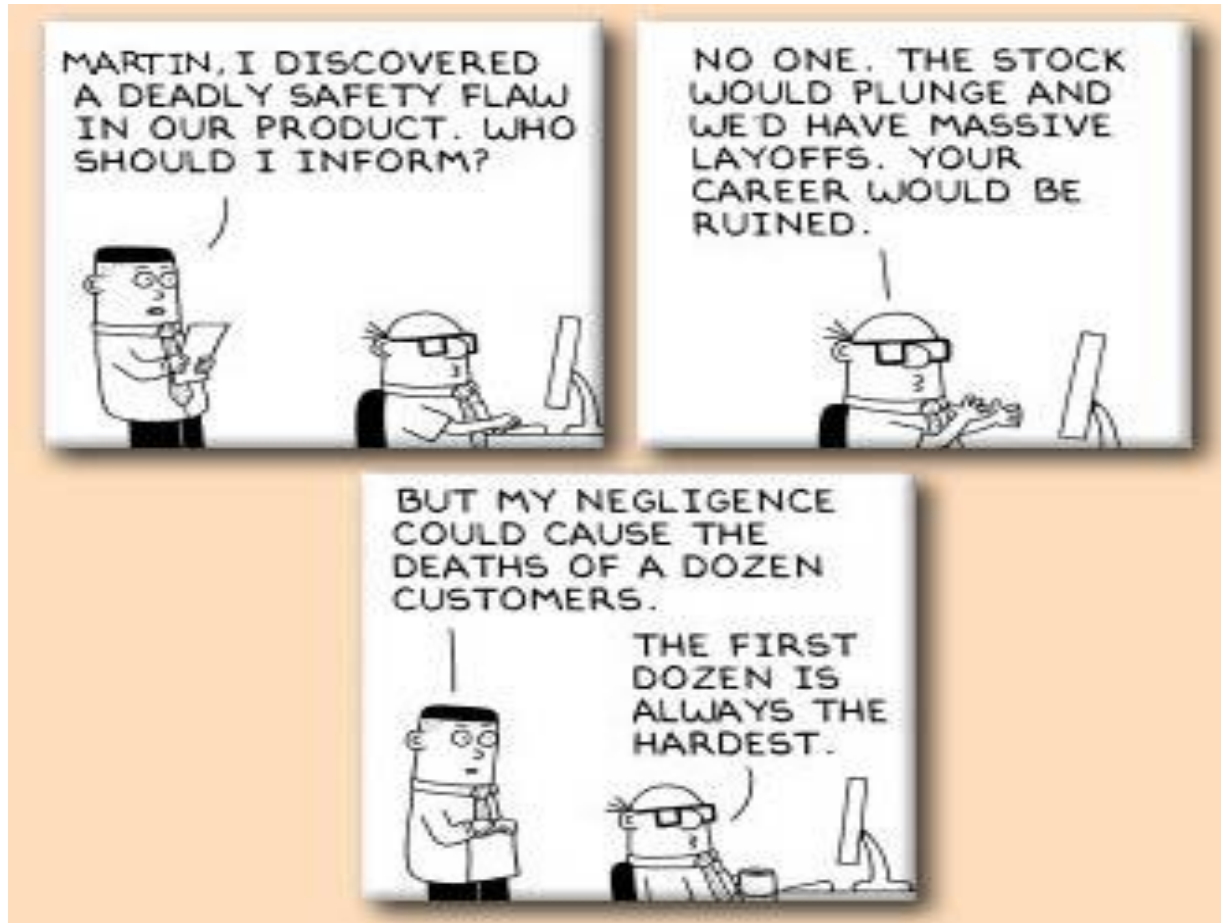
We are responsible to the communities in which we live and work
and to the world community as well.
We must be good citizens — support good works and charities
and bear our fair share of taxes.
We must encourage civic improvements and better health and education.
We must maintain in good order
the property we are privileged to use,
protecting the environment and natural resources.

Our final responsibility is to our stockholders.
Business must make a sound profit.
We must experiment with new ideas.
Research must be carried on, innovative programs developed
and mistakes paid for.
New equipment must be purchased, new facilities provided
and new products launched.
Reserves must be created to provide for adverse times.
When we operate according to these principles,
the stockholders should realize a fair return.



Business Ethics

[conflicts between profit and public interest]



The Four Categories of Ethical Issues in IT

- **Privacy Issues** (confidentiality) involves collecting, storing, and disseminating information about individuals
- **Accuracy Issues** (integrity) involves the authenticity, fidelity, and accuracy of information that is collected and processed
- **Property Issues** involves the ownership and value of information
- **Accessibility Issues** revolve around who should have **what kind of access** to information and whether they should have to pay for this access

Protecting Privacy



- **Privacy.** The right to be left alone and to be free of unreasonable personal intrusions
- Two rules have been followed fairly closely in court decision in most countries:
 - *The right of privacy is not absolute - privacy must be balanced against the needs of society*
 - *The public's right to know is superior to the individual's right of privacy*
 - US Patriot Act - DHS

US Patriot Act

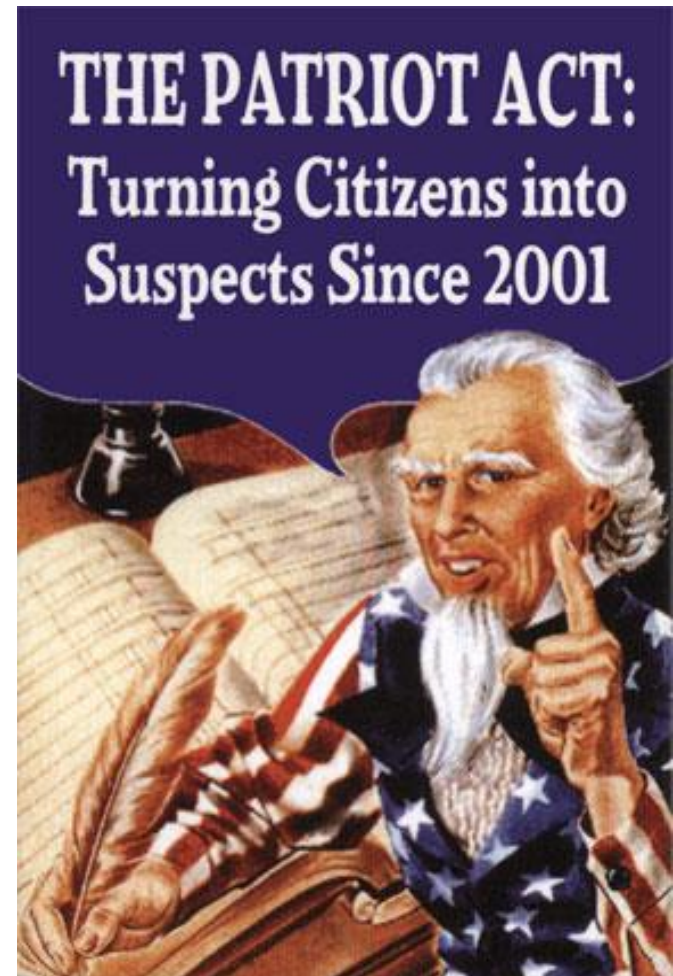
A graphic with a background of the American flag. The title "USA PATRIOT ACT" is in large, bold, white letters. Below it, the subtitle "Important Information About Opening A New Account" is in bold. The main text explains the government's need to fight terrorism and money laundering, requiring financial institutions to collect identifying information from new account holders. A section titled "What this means for you:" lists the specific information requested, such as name, address, date of birth, and driver's license.

USA PATRIOT ACT

**Important Information
About Opening A New Account**

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify and record information that identifies each person who opens an account.

What this means for you:
When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.



IT & Privacy – Hot Issues Today

- **Electronic Surveillance.** The tracking of people's activities, online or offline, with the aid of computers
- **Information on social media, Internet bulletin boards, newsgroups, directories, chat rooms, and blogs**
 - **Have you Googled your own name ?**
- **Personal Information in Databases -** Information about individuals is being kept in many types of databases: public & government, private, social, medical, banks, utilities, and credit-reporting agencies

NSA Communication Surveillance



- In everyday life, what ways do you pass on information about yourself ?





Information About Yourself

- **A better question might be: in what ways do you not pass on information**
- Think about all the ways you generate information about yourself that other people can use:
 - credit card purchases
 - telephone calls
 - cable TV viewing
 - e-mail & internet usage
 - magazine subscriptions
 - mail order purchases
 - banking transactions
 - video and other rentals
 - “Kroger” card





HOME

BROWSING THE INTERNET

That search engine you're using to find websites or information tracks your browsing activity. It then analyzes this behavior to target ads to you.

SHOPPING ONLINE

Amazon and other online retailers have made it an art form to track not only your purchasing patterns but also what items you viewed so they can recommend more products that align with your interests and needs.

LISTENING TO MUSIC

When you activate an Amazon Echo or Google Home speaker by voice, those companies record what you utter. Doc Searls, editor in chief at *Linux Journal*, calls smart speakers "a personal data fire hose squirting from your house."

WATCHING TV

Some smart TVs can collect your viewing data and other information. New models typically ask your permission first, but it's not always easy to understand what you're agreeing to. If you have an older set, it may be tracking you by default—you'd have to opt out.

Your Life

Urgent Care

RESEARCHING YOUR GENEALOGY

Businesses like 23andMe and Ancestry.com promise to reveal your genetic relatives based on the DNA from a saliva sample. But who's able to peek at that data? Recent criminal cases reveal that police are working with such services to gather information for investigations.

VISITING YOUR DOCTOR

Pacemakers, defibrillators and other medical devices are now often connected to your doctor or hospital, transmitting medical information.

Mug Puddle

SURFING THE WEB AT A COFFEEHOUSE

Beware of eavesdroppers on free Wi-Fi networks. "The person next to you could be using a tool called a packet sniffer to see what data you're sending to the websites you visit," says Ray Klump, professor and chair of computer science and mathematics at Lewis University.

SHOPPING AT A STORE

Those cards that get you discounts at stores and restaurants and other businesses are used to track your name, address and what you buy.

GETTING YOUR COMPUTER FIXED

Got a problem with your computer? The repair team at that big-box store can help. But recent reports revealed that employees at Best Buy were paid by the FBI to notify them of possible illegal content on customers' computers.

Clothing Zone

Electronics

DRIVING

E-ZPass and other toll transponders create a log of your locations. Also, speed or red-light cameras at key locations snap license plate numbers along with the date, time and location. And some auto insurance companies may want to track your driving with a device installed in your car that transmits data.

OUT AND ABOUT**RENTING A CAR**

Connecting your phone to the onboard electronics in a rental car could be risky. "Anyone who uses the car afterward may be able to go through the car's menus and see what calls you made, and they may even be able to find out your contact list," Klump says.

**DOING RESEARCH
AT THE LIBRARY**

"If you go to the library and use a public internet kiosk there and forget to log out, the data you saved and the websites you visited will be available to the next person," Klump says. Browsers offer a setting through which you can clear your history, logins and other info.

EXERCISING

The fitness tracker on your wrist collects data on your workouts, exercise routines and location. That information is shared with the manufacturers and can be synced with your social media accounts.

TAKING A WALK

Your phone's location service tracks you and may share that data with certain apps. Says Jeff Wilbur, technical director of the Online Trust Alliance: "We love the benefit of our smartphones as GPS or to utilize ride-sharing or similar location-based services, but by default those apps track and log a tremendous amount about your location history." Also, surveillance cameras are increasingly used in public places, to aid police investigations or monitor for suspicious activity.



Private Databases

- Credit data
- Medical data
- Memberships
- Subscriptions
- Banking
- Purchases & Rentals
- Telephone, Cable TV, Internet/E-Mail providers
- Employment



Privacy and Targeted Advertising

- The % of clicked on adds that result in a sale from a **targeted ad** (advertisements are placed so as to reach consumers based on various traits such as demographics, purchase history, or observed behavior) is **6.8%**, as opposed to a non-targeted ad rate of **2.8%**
- In 2005 40% of business web sites tracked viewers behavior, **that is now up to 85%**
- The privacy policy of most business websites say they only share your data with their subsidiaries – the median number of subsidiaries of the top 50 business websites is 93

Government Info

- Census Data
- Tax Data
- Social Security Data
- Criminal Data
- Medical Data
- Bankruptcy & Liens
- Permits
- Lawsuits
- Marriages/Divorces
- Welfare, Medicaid, Medicare
- Library Usage
- Voter Information
- Motor Vehicle Information
- Firearm Information
- Property Records
- Business Records

How to act...

- Best to act like your home, office, car, etc. is “bugged” all the time
- Best to act as if you are on camera all the time



Private Browsing - Anonymizer



1.800.921.2414 [Consumer Privacy](#) [Ntrepid Products](#)

[OVERVIEW](#) [USE CASES](#) [RESOURCES](#) [SUPPORT](#) [CONTACT US](#)

Ion disperses enterprise web scraping activity over our vast network of anonymous rotating IP addresses, allowing you to increase your data collection speed, avoid detection by targeted sites, and perform unrestricted deep-drill scraping. Ion is not only faster and safer, but is more reliable than other comparable solutions. Our high-speed, low latency IPs accelerate your data collection, with far more accurate and reliable results.

The Ion Advantage



Speed



Reliability



IP Quality

Our pricing model is bandwidth-based, giving you unlimited access to a vast pool of anonymous IPs and no data overage charges—EVER.

You'll never have to worry about keeping track of your usage or connections.

Epic Privacy Browser

 Epic's Encrypted Proxy is a free built-in VPN that protects your browsing history from your ISP & other data collectors and secures you on public WiFi.

 epic privacy browser

[Home](#) [Epic Key Features](#) [Blog](#) [Forum](#) [FAQ](#) [About Us](#) [Contact Us](#)

Why I need Epic

No Data Abuse

Your searches and browsing history are tracked and sold even sensitive searches for jobs and health conditions.



No Ads

Tired of ads using your personal data following you around the internet?

Exposed: Shocking Truth
Behind Getting Pregnant
See the system thousands of women are using. More here.



No Spying

 22 Trackers
 31 Trackers

Lower Price

\$1770 vs. \$2116 for a NYC-AUS flight.

"[Consumer Reports] found the cleared browser offered fares... from \$1,770 to \$1,950 [vs.] \$2,116 [in the uncleared browser]."

USA Today

The world's only private and secure web browser blocks ads, trackers, fingerprinting, cryptomining, ultrasound signaling and more. Stop 600+ tracking attempts in an average browsing session. Turn on network privacy with our free VPN (servers in 8 countries).

 **Download Epic Now** 

Epic is FREE and installs in less than a minute.

We believe what you browse & search online should always be private. In incognito mode, you're still being tracked. Join over one million users who've chosen privacy. For Mac & PC.

As seen in:



Epic (con't)

 You're still **tracked** in Incognito mode.

Your Browsing History is:					
Deleted from your computer					
Protected from:					
Your ISP					
Your Government					
Hundreds of Data Collectors					
Your Employer					

* Epic provides full protection with the encrypted proxy turned on.
** Firefox and Apple use Google services and receive over \$300 million and \$3 billion from Google respectively.

Epic (con't)

Blocking cookies? Using a VPN? You're still being tracked.

You're tracked not just with cookies but also via device fingerprinting, most prevalently image canvas data which only Epic blocks.

A simple webrtc function can leak your actual IP address even if you're using a VPN. Epic protects you.

Epic lets you spy on the spies.
See who's tracking you in your other browsers.
See the trackers Epic blocks at each website you visit.



Government Info Laws

- Governments (both Federal, local, and state) maintain a lot of information on you.
 - By law this is normally public information and anyone can have access to it (license plate example)
- There are over 1000 Federal and State laws concerning information privacy

Major US Privacy Legislation

- Fair Credit Reporting Act (1970) - allows individuals access to their credit records, to receive free copies, and to challenge the contents
- Freedom of Information Act (1968) - Allows citizens to get access to data that has been gathered by federal government – however one needs to know specifics, pay charge, and wait.....

Major US Privacy Legislation (con't)

- Privacy Act of 1974 - Allows people to determine what information is collected about them by Federal government, to prevent records obtained for one purpose from being used for another, to have access to and get copies of information on them, to correct records, to file civil suits for damages
- Problems:
 - 17 percent of government agencies are exempt
 - Government disorganization and bureaucracy prevent individuals from learning about most data
 - Government employees sell and use information

Right to spy ?

- Does your employer (or school) have to right to access information and usage of your work computer?
- Does your employer (or school) have to right to access information and usage of **your own** computer (or cell phone) at the workplace?
- Does your parent have to right to access information and usage of your computer at home?
- Does your spouse have to right to access information and usage of your computer at home?



Major US Privacy Legislation (con't)

- Electronics Communications Privacy Act of 1986
 - Protects the privacy of electronic messages sent through *public* networks
 - Not through private networks (ie *your employer*)
 - Not in your home (ie *your parent and/or spouse has access rights*)
- Digital Telephone Act of 1994 requires that all telecommunications equipment be built so that the government can tap into it

Major US Privacy Legislation (con't)

- Telecommunications Act of 1996 - is the first major overhaul of telecommunications law; the goal of this new law is to let anyone enter any communications business -- to let **any communications business compete** in any market against any other
- Communications Decency Act (CDA) - was the first notable attempt by the United States Congress to **regulate pornographic** material on the Internet

Major US Privacy Legislation (con't)

- Health Insurance Portability and Accountability Act (**HIPAA**) - is US legislation that provides data privacy and security provisions for **safeguarding medical information**
- Fair and Accurate Credit Transaction Act (**FACTA**) - is an amendment to FCRA (Fair Credit Reporting Act) that was added, primarily, to **protect consumers from identity theft** and stipulates requirements for information privacy, accuracy and disposal
- Children's Online Privacy Protection Act (**COPPA**) is a law created to protect the **privacy of children** under 13. The Act was passed by the U.S. Congress in 1998 and took effect in April 2000

Social Media & Privacy

- 24 million Facebook users leave their profiles mostly public
- 73% of social media profiles can be found thru a public search engine
- 77% of social network users do not restrict access to their photos
- 70% of employers now use social web sites to check on job candidates
- 33% of employers have found information that caused them not to hire a candidate
- Facebook profile now being used to check rental applications, credit applications, insurance applications, etc.

Social Intelligence



55% of Millennials are willing to share their data in exchange for discounts

Which Apps Allow False Information

		POLITICS/ SOCIAL	HEALTH/ CORONAVIRUS	VOTING/ CENSUS	MANIPULATED MEDIA
	FACEBOOK	●	●	X	X
	INSTAGRAM	●	●	X	X
	YOUTUBE	●	●	X	●
	TWITTER	●	●	X	●
	PINTEREST	●	X	X	X
	REDDIT	●	●	●	X
	SNAPCHAT	●	X	X	X
	WHATSAPP	●	●	●	●
	TIKTOK	●	X	X	X
 ALLOWED  SOMETIMES X PROHIBITED					

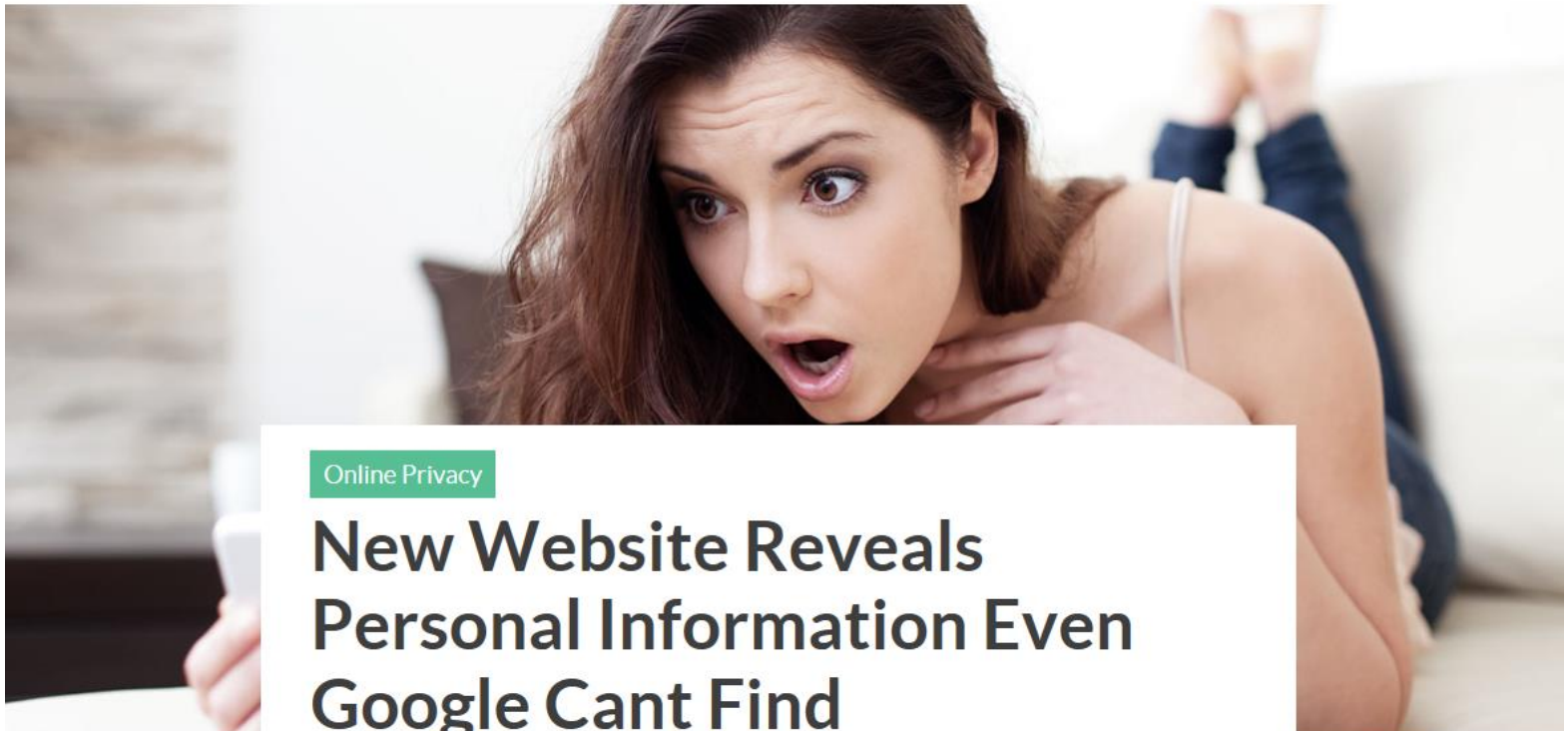
Social Media & Jobs

- Companies have long used criminal background checks, credit reports and even searches on Google and LinkedIn to probe the previous lives of prospective employees
- **Now, many companies are requiring job candidates to also pass a social media background check**
- Social Intelligence scrapes the Internet for everything prospective employees may have said or done online in the past decade or so
 - Then it assembles a dossier with examples of professional honors and charitable work, along with negative information that meets specific criteria: online evidence of racist remarks; references to drugs; sexually explicit photos, text messages or videos; flagrant displays of weapons or bombs and clearly identifiable violent activity

www.truthfinder.com



START HERE - Try searching a friend, relative, celebrity, yourself, or someone else you might know...



Online Privacy

New Website Reveals Personal Information Even Google Cant Find

U.S. tech giants have enormous influence over what we buy, read, see, and think. But is their market power illegal? At a July 29 House hearing, lawmakers leveled monopoly-abuse accusations at the leaders of Amazon, Apple, Facebook, and Google. We sift through the charges, compile the evidence, summarize the CEOs' defenses, and ask experts whether the lawmakers made their case. — *David McLaughlin, Ben Brody, and Naomi Nix*

Amazon



THE ALLEGATION

Amazon.com Inc. uses predatory pricing to crush rivals. In 2009 it decided Diapers.com was a significant threat and started a price war against it. Amazon slashed prices so much it lost \$200 million in a month on diapers. It then acquired Diapers.com owner Quidsi Inc., cut promotions and discounts, and ultimately increased prices, said Democratic Representative Mary Gay Scanlon of Pennsylvania.

THE EVIDENCE

In an internal email, North American consumer sales chief Doug Herrington said Amazon needed "to match pricing on these guys no matter what the cost."

THE CEO DEFENSE

At the hearing, Chief Executive Officer Jeff Bezos said he didn't remember raising prices after the Quidsi deal. "This was 11 years ago," he said, adding that price discounts to attract customers are a traditional retailer tactic and that customers had many other options for diaper purchases.

THE LEGAL ANALYSIS

Predatory pricing cases are difficult. The government would have to show that Amazon set diaper prices below acquisition costs and that, once a rival was driven out of business, Amazon was able to recoup losses by raising prices above a competitive level. "The hardest part of this burden is this recoupment requirement," says George Washington University law professor William Kovacic. "Show me how consumers are worse off."

Apple



THE ALLEGATION

Apple Inc. is an unfair gatekeeper to its App Store, controlling the fate of developers by deciding which apps get in and sometimes playing favorites. Democratic Representative Val Demings of California said Apple's policies allowed it to pick app winners and losers. "Apple rules mean Apple apps always win," she said.

THE EVIDENCE

Apple agreed in 2016 to halve its typical 30% App Store fee for Amazon in a deal to put its Prime Video app on Apple's mobile devices and TV set-top box. The companies agreed to a 15% revenue share for customers who signed up through the app and no share for users who subscribed elsewhere. Internal emails also show that CEO Tim Cook promised to fast-track approvals for apps from China's Baidu.

THE CEO DEFENSE

Cook said access is "very wide," to the App Store. "There's fierce competition for developers, and we want every app" on the platform, which has about 1.7 million available. He equated the competition to attract developers to a "street fight for market share in the smartphone business." Cook said Apple has never increased the commission it charges developers, and all apps are treated equally.

THE LEGAL ANALYSIS

Just charging developers a high commission isn't enough to bring an antitrust case, says Hal Singer, a managing director at consulting firm Egon One. There needs to be evidence of some restraint that harms competition.

Facebook



THE ALLEGATION

Facebook Inc. uses "copy, acquire, and kill" against rivals. It bought Instagram in 2012, seeing the site as an emerging threat. In 2014 it bought WhatsApp, a rival to its Messenger. Democrat Pramila Jayapal of Washington said Facebook identified Instagram as a competitive threat "and told them that if they didn't let you buy them up, there would be consequences."

THE EVIDENCE

Emails and texts show that CEO Mark Zuckerberg asked former Chief Financial Officer David Ebersman in February 2012 about buying Instagram and Path, a now-defunct social media company. Zuckerberg said they had established "meaningful" brands, and "if they grow to a large scale they could be very disruptive to us." He agreed that part of his motive in buying Instagram was to "neutralize a potential competitor."

THE CEO DEFENSE

Zuckerberg said Instagram succeeded because Facebook invested in it. "With hindsight it probably looks like, obvious that Instagram would have reached the scale that it has today, but at the time it was far from obvious."

THE LEGAL ANALYSIS

Jennifer Rie, an antitrust expert at Bloomberg Intelligence, says a monopoly-abuse case might succeed, but forcing Facebook to divest Instagram would be tough, unless the U.S. can prove there's been an actual loss to competition that needs restoring. That will be difficult to show given Instagram's current success and uncertainty about any independent future.

Google



THE ALLEGATION

Democrat David Cicilline of Rhode Island, who chairs the House antitrust subcommittee, fired off the hearing's first question to Google CEO Sundar Pichai: "Why does Google steal content from honest businesses?" Cicilline said the company uses that content to create a "walled garden" and to keep users on Google properties rather than directing them to sites that originated the information or offer more relevant data.

THE EVIDENCE

Cicilline cited an internal Google memo from 2006 that observed other websites were getting "too much traffic," so Google decided to "put an end to that."

THE CEO DEFENSE

Pichai disagreed with Cicilline's "stolen content" characterization. He said Google supports 1.4 million small businesses with more than \$385 billion in economic activity. Pichai also said Google conducts itself "to the highest standard," adding that it has numerous competitors, including Amazon, where "over 55% of product searches originate."

THE LEGAL ANALYSIS

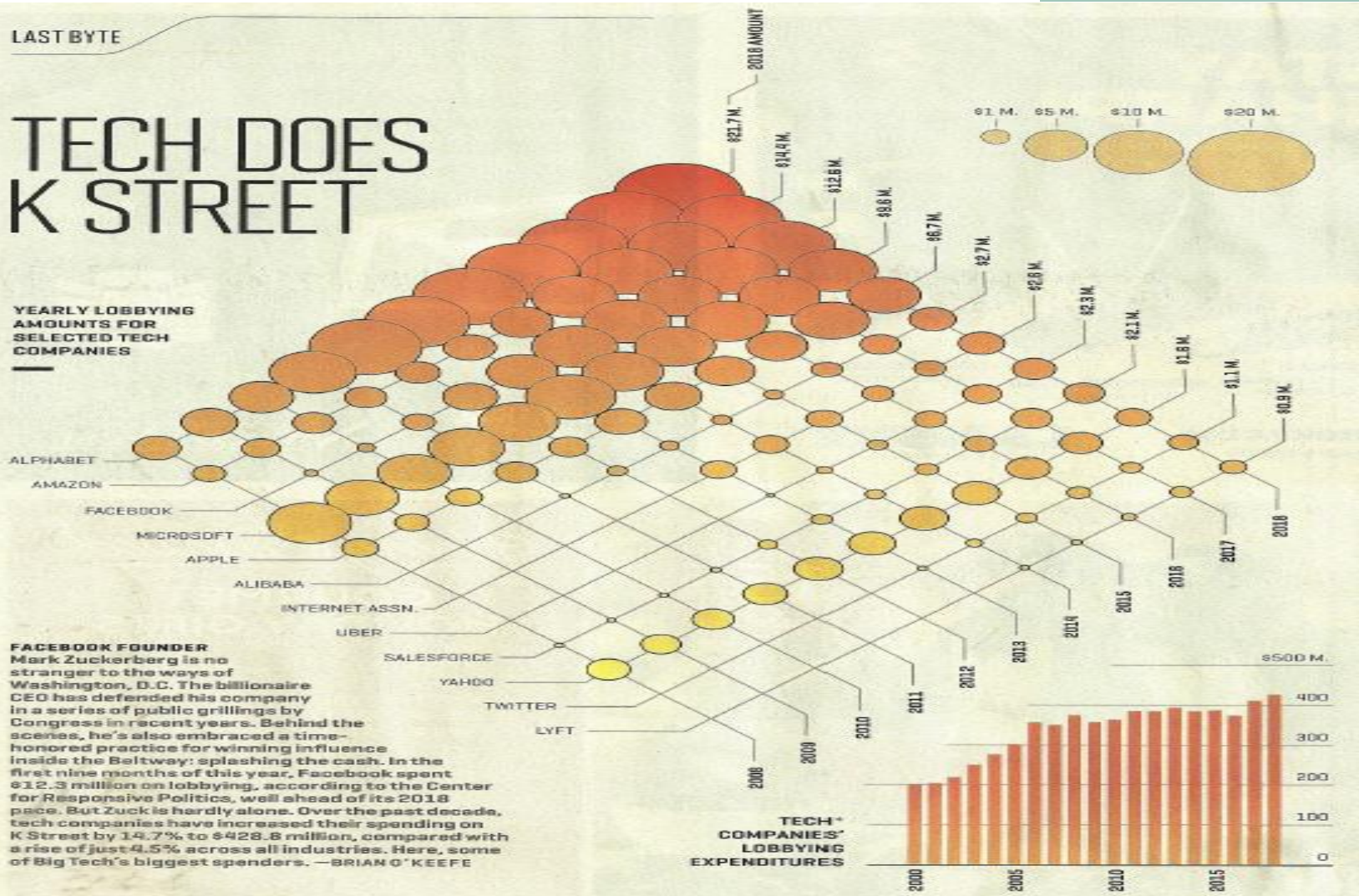
An antitrust challenge against Google could have a shot at success, says Bloomberg's Rie, if it could show the company's actions are excluding or substantially foreclosing rivals from access to the market. A case could claim that Google, without legitimate business justification, demoted rivals' content in search results so that users couldn't readily see it.

Lobbying by Tech Companies

LAST BYTE

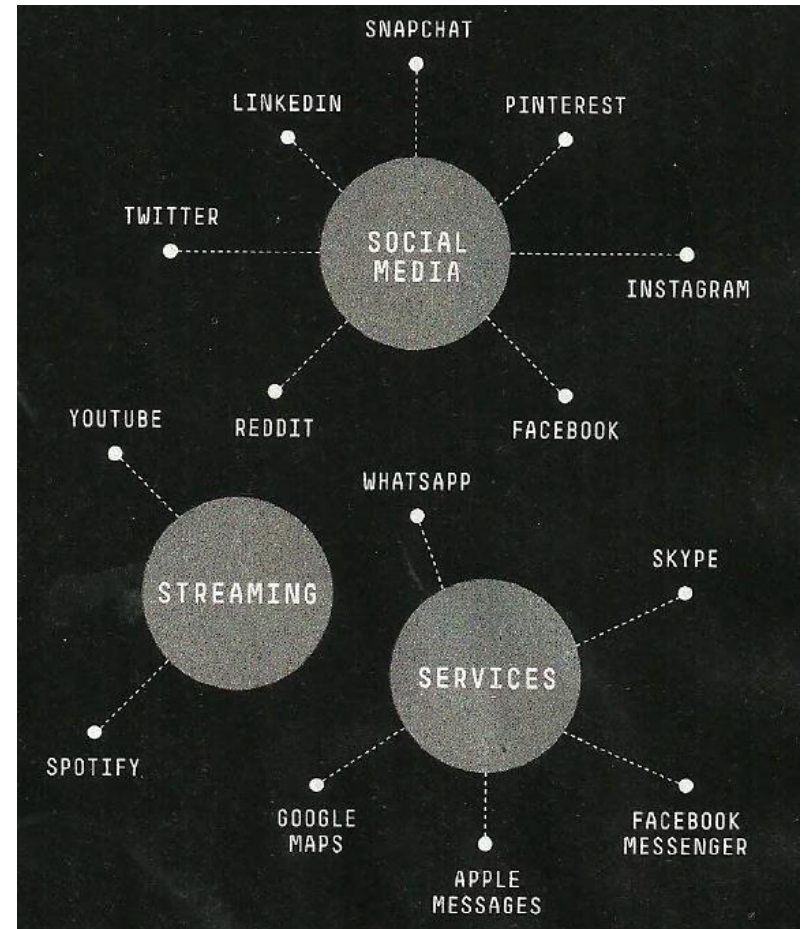
TECH DOES K STREET

YEARLY LOBBYING AMOUNTS FOR SELECTED TECH COMPANIES



Dark Patterns

- The US is considering a “Detour Act” to prevent “**dark pattern**” practices at social media web sites with over 100 million monthly active users



Dark Patterns (con't)

► PRIVACY PIRACY

Social platforms release more information to brokers than you realize. Also known as “Privacy Zuckering,” after Facebook’s CEO.

FOR EXAMPLE...

Facebook shares user data with advertisers by default. Users must change settings manually to opt out.

► MISDIRECTION

Page or app design purposefully focuses your attention on one thing to distract your attention from another.

FOR EXAMPLE...

Airbnb displays “per night” prices for listings, but other expensive line items such as cleaning, service fees, and tax aren’t shown until the booking process.

Dark Patterns (con't)

▶ DISGUISED ADS

Advertisements are cloaked as other kinds of content or navigation, in order to elicit a response from you.

FOR EXAMPLE...

Although Google's advertising platform has regulations against them, some ads it displays use fake "download" buttons to trick users into clicking on them.

▶ BAIT AND SWITCH

Software entices you to do one thing, but an undesirable thing happens instead.

FOR EXAMPLE...

Microsoft was criticized in 2016 when users noticed that hitting the X on a software update pop-up would actually download an app instead of closing the window.

Dark Patterns (con't)

► CONFIRM SHAMING

The option to decline or opt out of a function or service is worded in such a way as to make users second-guess themselves.

FOR EXAMPLE...

To cancel Amazon Prime, users have to push buttons that read "Cancel membership and end benefits" and "I do not want my benefits."

► FRIEND SPAM

A site asks for your email or social media permissions under false pretenses, then spams your contacts in a message claiming to be from you.

FOR EXAMPLE...

LinkedIn settled a class action lawsuit in 2015 for spamming users' entire email contact lists when they clicked an "add to your network" button while signing up.

Censorship

- Types of Information on the Web
 - **Public information** is posted by an organization, public company, or public agency
 - **Censored** for public policy reasons
 - **Censored** if the content is deemed offensive to a political, religious, or cultural group
 - **Private information** is posted by a private corporation or person
 - **Uncensored** because of constitutional freedom of expression

Section 230

- **Section 230** says that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"
- Dates back to 1996
- However now Section 230 is being blamed for enabling the **worst aspects of social media such as fake news, terrorist propaganda, revenge porn, promotion of dangerous and defective products, bullying, election interference, etc.**

Censorship (con't)

- Restricting access to the Web
 - Countries such as China, Russia, Myanmar (Burma), and Singapore **restrict or forbid their citizens' access to some/all of the Web**
 - Parents use programs such as CyberPatrol, CyberSitter, Net Nanny, and SafeSurf to **prevent children's access to Web sites**
 - **Net Neutrality**: Internet service providers (ISPs) and government agencies should treat all data on the Internet equally – **latest court ruling says that the while feds do not have to enforce net neutrality, they cannot prevent states from doing so**

Compromises to Intellectual Property

- **Intellectual property:** Property created by individuals or corporations which is protected under *trade secret*, *patent*, and *copyright* laws
- **Trade secret:** Intellectual work, such as a business plan, that is a company secret and is not based on public information
- **Patent:** Document that grants the holder exclusive rights on an invention or process for 20 years or so...



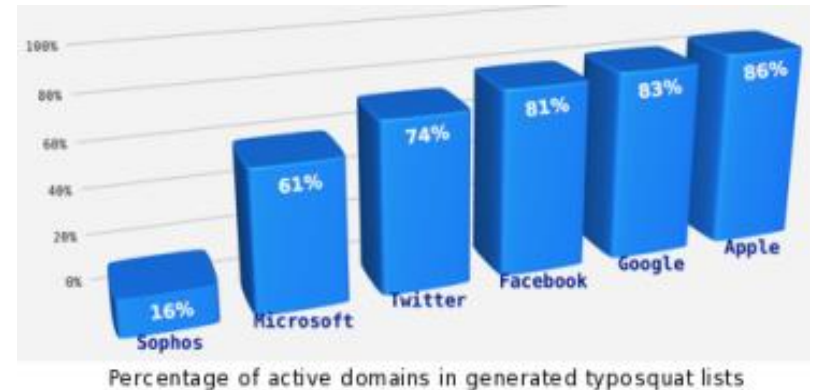
Compromises to Intellectual Property (Continued)



- **Trademark:** protects product names and identifying marks
- **Copyright:** Statutory grant that provides creators of intellectual property with ownership of the property for life of the creator plus 70 years or so
 - 1980 revisions to the Copyright Act of 1976 **include computer programs**
- **Fair Use Doctrine:** exception to the copyright law that allows the use of copyrighted material for certain purposes
- **Piracy:** Copying a software program without making payment to the owner

Intellectual Property (con't)

- Cybersquatting
 - Registering, selling, or **using a domain name** to profit from someone else's trademark
- Typosquatting
 - Relies on typographical errors made by Web users when typing a Web site address into a Web browser
 - Variation of cybersquatting
 - Called URL hijacking

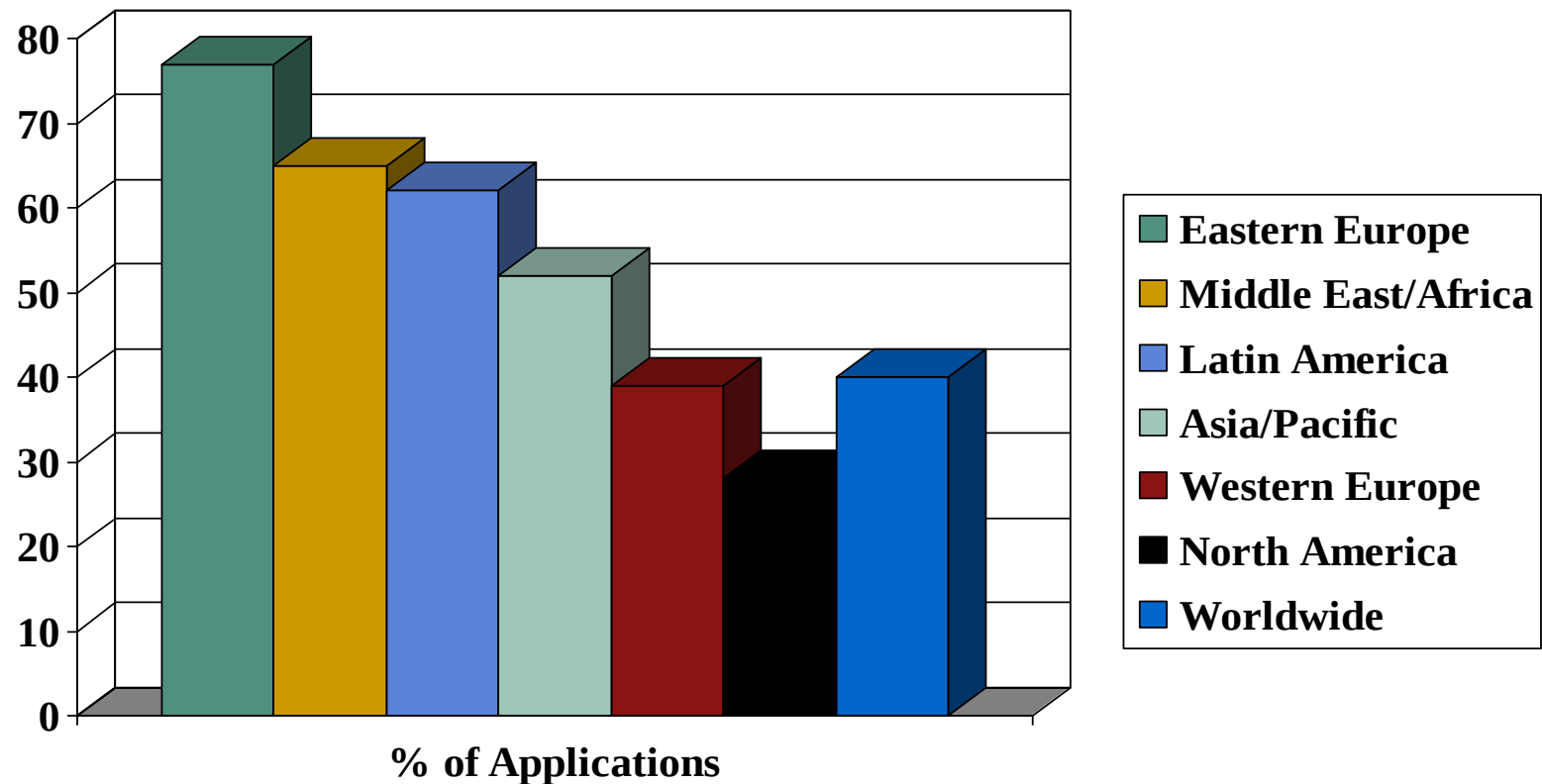


- What % of worldwide application software installs involve pirated software ?





Worldwide - 40% of Ap's are Pirated



SIIA

- The *Software Publishers Association (SPA)* was founded in 1984 with 24 members
- The membership later grew to a thousand small companies, and in 1999 it was merged with the (*SIIA*) to form the *Software & Information Industry Association*
- If you illegally copy software, it is Federal crime subject to fine of up to \$100,000 per incident !
- When you copy software you lose the benefits of documentation, upgrades, support, etc.
- When you copy software, you are depriving the author's of their fair compensation and hurting the industry
- SIIA "audits"
 - Like IRS, one is guilty until proven innocent

- SIIA “Hotline”

- 800 - 388 – 7478

- Who makes most of the calls to the SIIA hotline?





■ Disgruntled employees



Illegal Downloads

Minnesota Mom Hit With \$1.5 Million Fine for Downloading 24 Songs

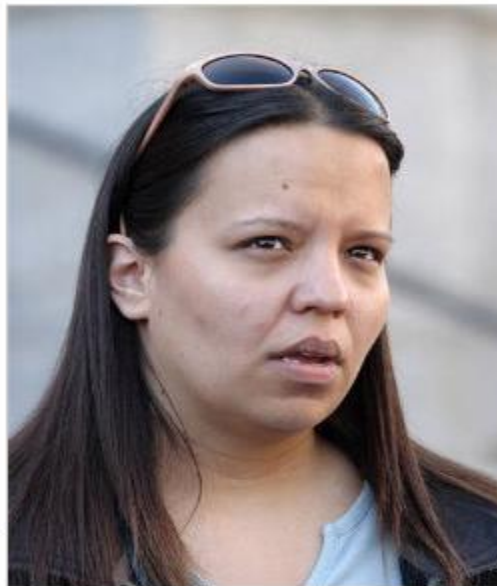
Posted Thu Nov 4, 2010 10:38am PDT by Daniel Kreps

in Amplifier

 Share 34K  retweet 976

What's the value of a song? Jammie Thomas-Rasset has spent the last few years in court debating that question. The Minnesota mother of four is being penalized for illegally downloading and sharing 24 songs on the peer-to-peer file-sharing network Kazaa in 2006, but how much she owes the record labels has been in question. The jury in her third trial has just ruled that Thomas-Rasset should pay Capitol Records \$1.5 million,

CNET reports, which breaks down to \$62,500 per song. It's a heavy penalty considering the 24 tunes would only cost approximately \$24 on iTunes, which was Thomas-Rasset' argument, too.

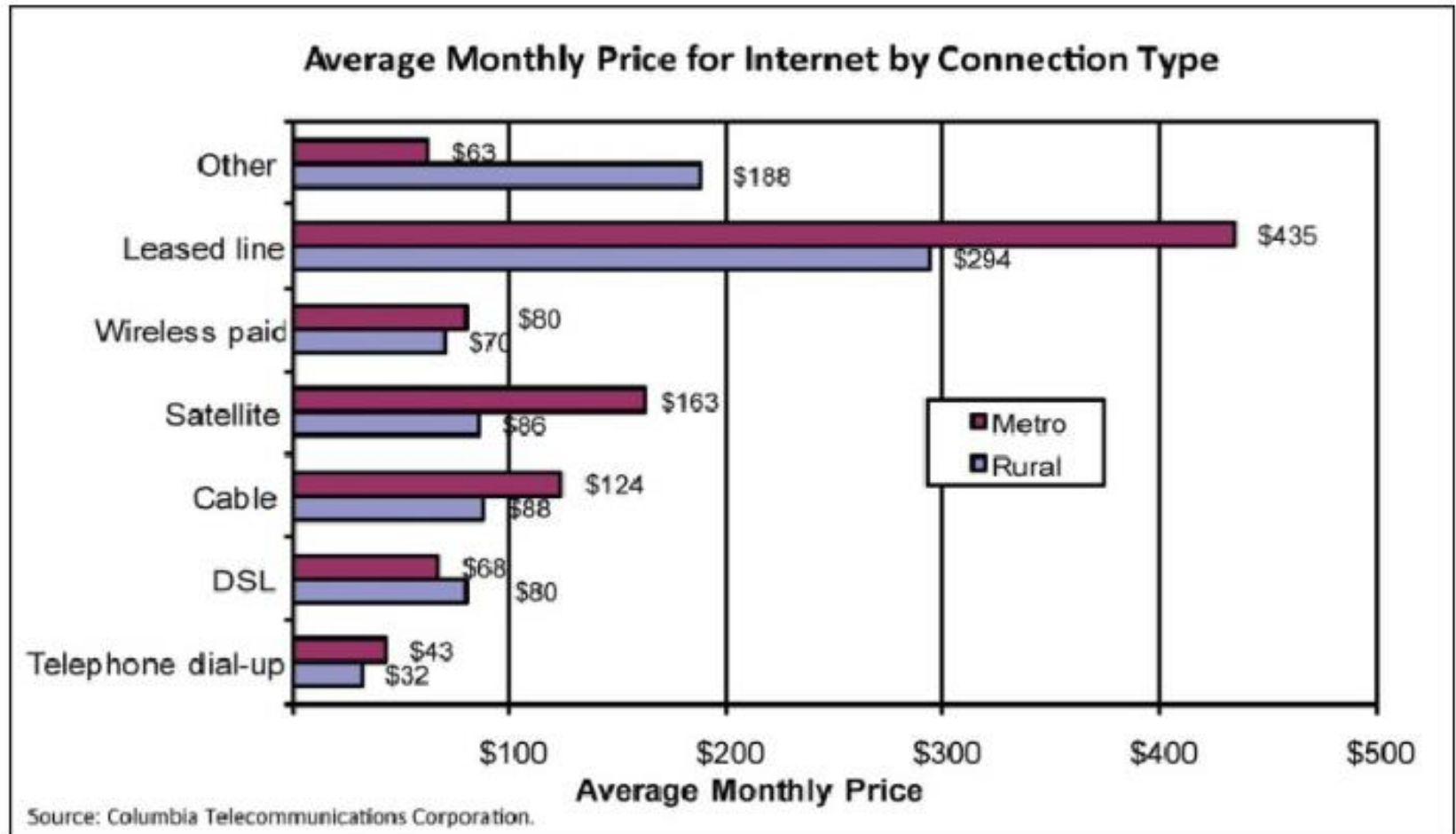


Social Divisions and the Digital Divide

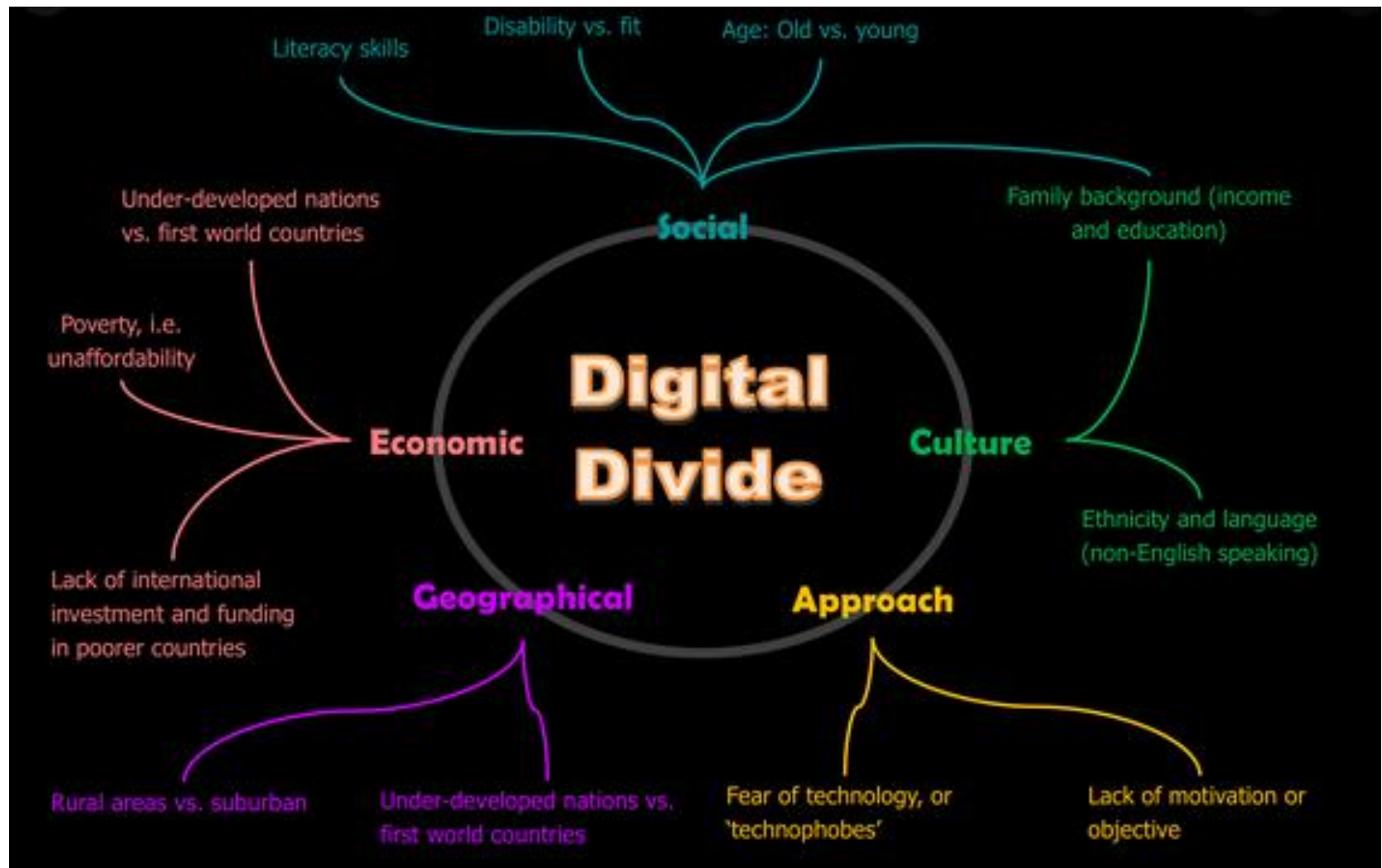
- **Digital divide**: created between the information rich and the information poor by information technology and the Internet
 - Computers still are not affordable for many people
 - Increasing funding for computers at schools and public places helps offset the divide
 - Internet connections are still **not available** everywhere
 - Internet connections are still **not affordable** for all



Digital Divide (con't)



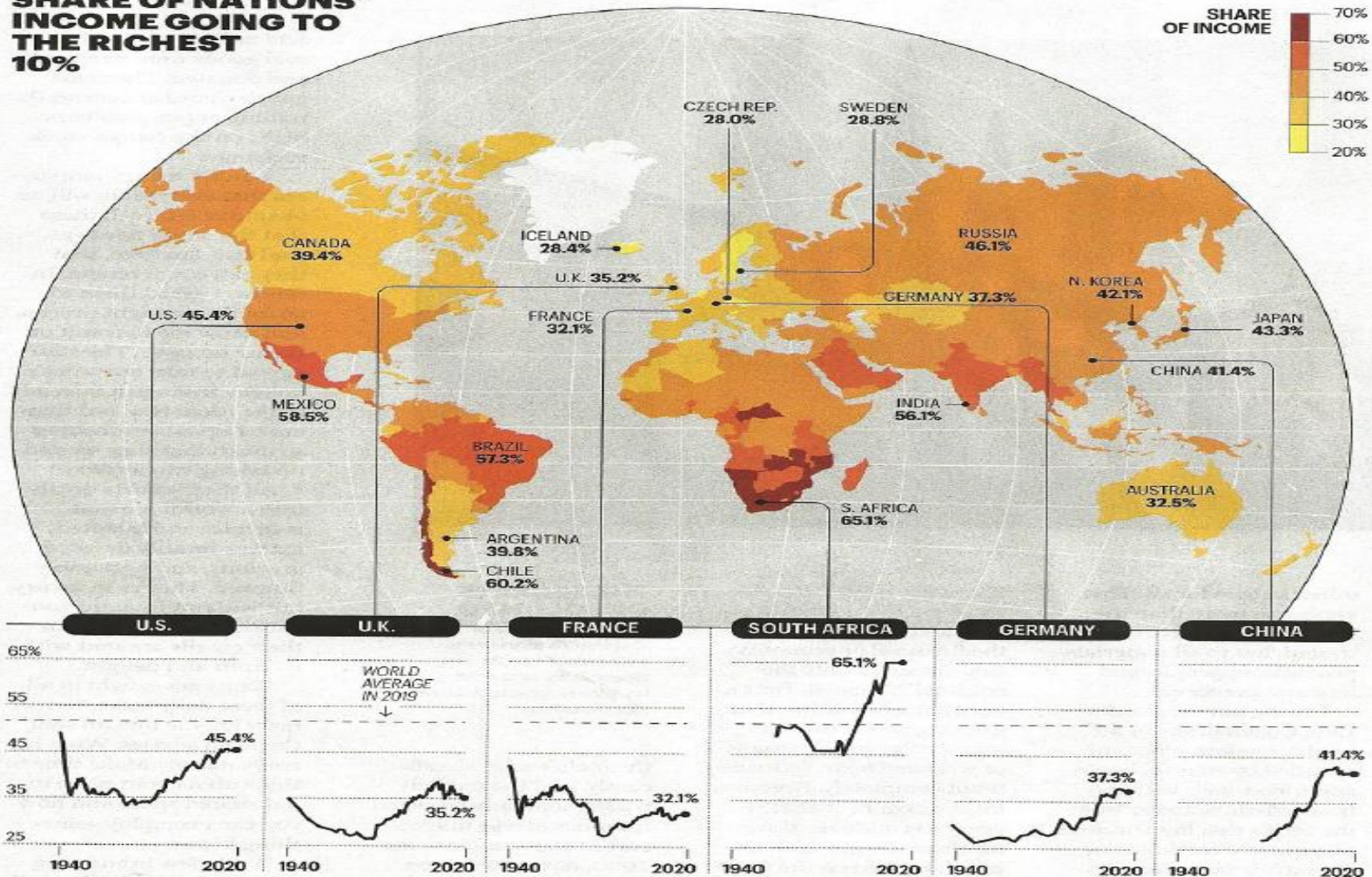
Digital Divide (con't)



The Rich are Getting Richer

[Digital Divide is one Cause]

SHARE OF NATIONS' INCOME GOING TO THE RICHEST 10%



Green Computing

- Promotes a sustainable environment and **consumes the least amount of energy**
- Involves design, manufacture, use, and disposal of computers, servers, and computing devices with **minimal impact on the environment**
- Requires cooperation of both private and public sectors



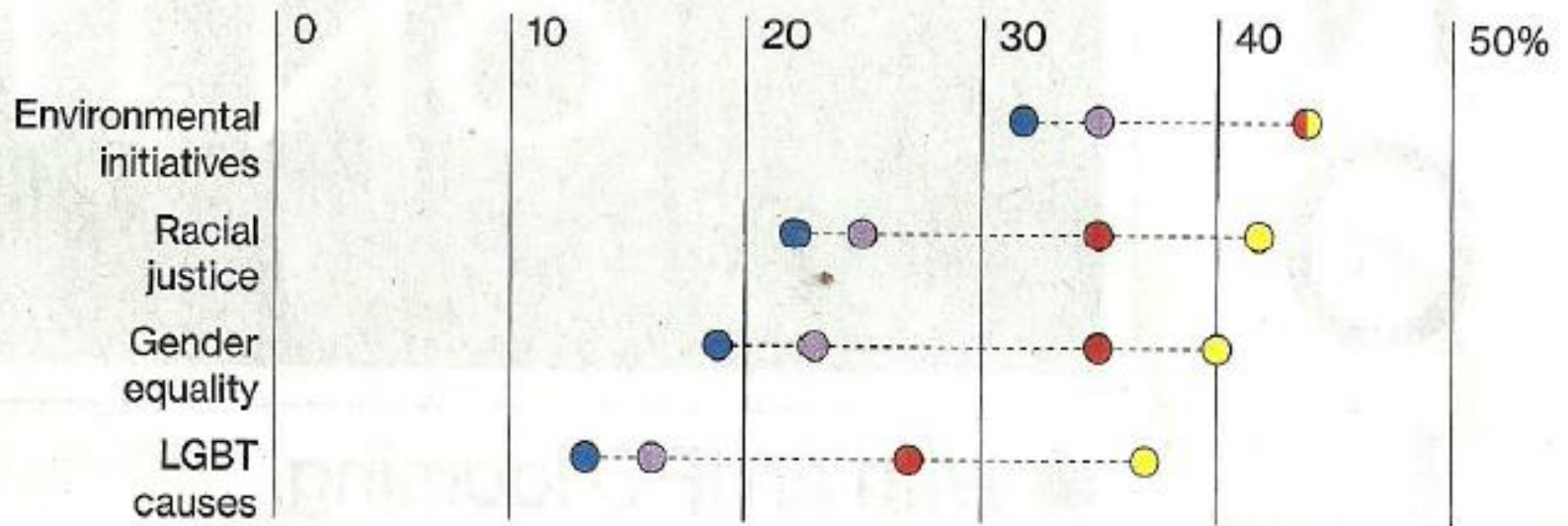
Green Computing (con't)

■ Ways to achieve green computing

- Designing products that last longer and are **modular in design**
 - Parts can be upgraded without replacing the entire system
- Designing search engines and computing **software that are faster and consume less energy**
- Replacing underutilized smaller servers with one large server using a **virtualization technique**
- Using computing devices that **consume less energy and are biodegradable**
- Allowing certain employees **to work from their homes**
- Conducting **meetings over computer networks** to reduce business travel
- Using **cloud computing**
- **Recycling** computer-related materials

Generations and Social Issues

Share of respondents by generation who say they'd pay more for a product if the brand or retailer promotes...



● Boomers
54-72 years old

● Generation X
38-53

● Millennials
22-37

● Generation Z
18-21

The Growth of Telecommuting



- Telecommuting has gained popularity since the late 1990s because:
 - Lowers corporate overhead since workers who are at home don't take up office space lowering facilities costs
 - some companies now have a large portion of their staff without any formal "office"
 - Companies like Cisco have gone from 200 square feet per employee to 50 and 60 square feet
 - Workers who are given increased flexibility are generally more productive and express higher levels of job satisfaction
- 2/3's of Cisco employees occasionally work from home. The policy has saved the company \$1M in monthly expenses, while workers prefer to set their own schedules and work in more comfortable surroundings.

Enabling Factors for Telecommuting

- Three factors support the growth of telecommuting growth:
 - **Work is increasingly knowledge-based** so workers don't need to be "at work" to do their jobs
 - More **powerful computers plus cheaper telecommunications** make it possible for telecommuters to be connected to corporate networks at higher data rates from anywhere
 - **Network hdw/sft improvements** enable workers to shift their work to accommodate their lifestyles, especially parenting or living in distant locations far from the office.



Telecomputing Benefits



Potential Benefits

Can care for small children or elderly parents and spend more time with family

Have fewer restrictions on clothing for work, thereby saving the expense of work wear

No commute, so distance and time factors are reduced as well as the effects of car emissions on air quality

Able to work in more pleasant surroundings

Increased productivity

Decreased neighborhood crime because of more people being home during the day

Easier work environment for employees with disabilities

Reduced costs for office space and utilities

Reduced employee turnover and absenteeism

Able to find and hire people with special skills, regardless of where they are located

Fewer interruptions from coworkers

- Despite the advantages of telecommuting from both the employers and employee's perspectives, what are some of the potential work problems with telecommuting ?



Don't look ahead ...



Telecomputing Drawbacks

Potential Drawbacks

Can become a workaholic (no hard boundaries between “at work” and “at home”)

No regulated work routine



Less interaction with coworkers

No separation between work and home life

Potential legal issues about workers' injuries

Family interruptions and household distractions

Lack of necessary supplies or equipment

Could create a two-tiered workforce—telecommuters and on-site workers—that affects promotions and raises

Telecommuters May Go Nowhere – Career Wise

(Los Angeles Times 1/17/2007)

- Maybe Woody Allen may have been right, that “80% of life really is just about showing up”
- At least that's what many executives seem to think about people who work from home
- Telecommuters are less likely to get promoted than peers who head into the office every day, according to a global survey of 1,300 executives.
- Executives may also be concerned about promoting a hardcore telecommuter to a management position in which face time with employees is essential. . .
- 61% dinged telecommuters as being poorer bets for advancement
- “If you're not cultivating the right network of people, you won't move up in any setting, whether you're telecommuting or not”

Telecommuting (con't)

- Six telecommuting questions companies need to answer:
 - Is full time telecommuting a smart decision?
 - How will you define and measure performance?
 - Will creativity suffer?
 - How will telecommuting affect collaboration?
 - What about employees “left behind” at the office?
 - Do you have an exit strategy?

- Are there some sociological problems or issues concerning working remotely, telecommuting, or the technologies involved ?



Don't look ahead ...



Sociological Problems

- People driving while on the phone
- Annoyances of mobile phones (ringing at inappropriate times/places)
- People becoming “socially disconnected”
- Over-indulgence (eating, smoking and other things not done as much as if one were in the workplace)
- Medical issues with wireless communications (i.e. brain damage due to radiation, etc. ?)
 - Mobile 5G will bring increased radiation

Are mobile phones dangerous?

Yes	No
Radio waves given off by mobiles can heat up body tissue, having damaging effects	Radio waves are not powerful enough to cause heat damage to the body
Magnetic fields created by mobile phones can affect the way that your body cells work	The magnetic fields are incredibly small, and so unlikely to affect cells in our body
People who make long mobile phone calls sometimes complain of fatigue, headaches, and loss of concentration	The same results have never been reported in laboratory conditions and may be due to other factors in modern lifestyles
Mobile phone users are 2.5 times more likely to develop cancer in areas of the brain adjacent to their phone ears	Researchers admit it's unclear this increase is linked to using mobiles
The International Agency for Research on Cancer found a link between childhood cancer and power lines. Like mobile phones, power lines also emit radiation	The radiation produced by powerlines is a different kind of radiation, with much more energy than that coming from mobile phones
Radio frequency waves similar to those in mobile phones altered the gene expression in nematode worms	Worms are not humans, there is no guarantee that our brain cells will behave in the same way

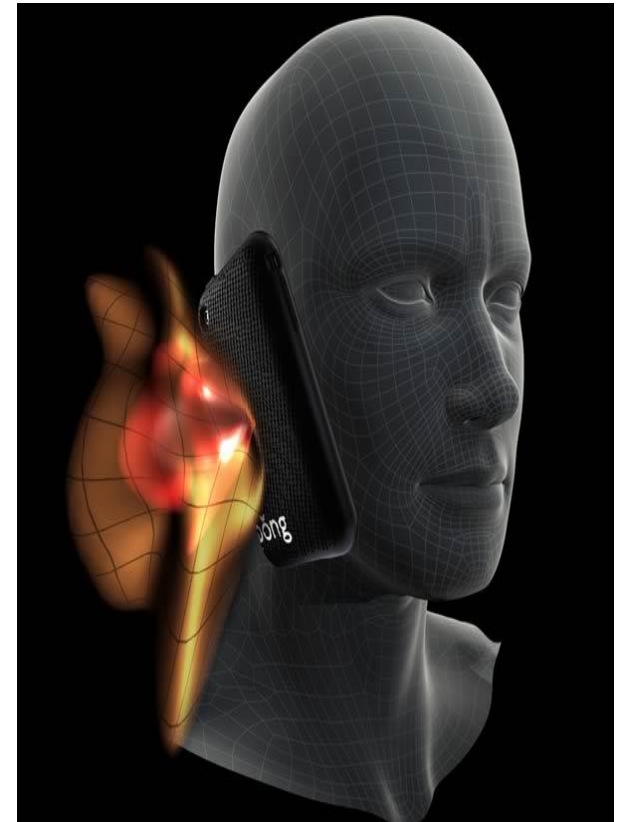


A 2010 medical study proved that cell phone radiation alters brain activity !

A 2015 medical study found that cell radiation causes cancer in rats !

Ways to Reduce Cell Phone Radiation

- Use a wired headset – that is less radiation than a Bluetooth headset
- Use SMS texting instead of voice
- Don't use the cell phone as an alarm clock – next to your bed
- Be careful with radiation hot spots – cell phones put out more radiation when the signal is weaker such as in rural areas, elevators, etc.
- Use a radiation blocking case
- Don't live or work near a cell tower



Should You Be Snuggling With Your Cellphone?

New York Times – 11/2010

WARNING: Holding a cellphone against your ear may be hazardous to your health. So may stuffing it in a pocket against your body.

I'm paraphrasing here. But the legal departments of cellphone manufacturers slip a warning about holding the phone against your head or body into the fine print of the little slip that you toss aside when unpacking your phone. Apple, for example, doesn't want iPhones to come closer than 5/8 of an inch; Research In Motion, BlackBerry's manufacturer, is still more cautious: keep a distance of about an inch.

"Most cancers have multiple causes," she says, but she points to laboratory research that suggests mechanisms by which low-energy radiation could damage cells in ways that could possibly lead to cancer.

Children are more vulnerable to radiation than adults; radiation that penetrates only two inches into the brain of an adult will reach much deeper into the brains of children because their skulls are thinner and their brains contain more absorptive fluid

Henry Lai, a research professor in the bioengineering department at the University of Washington, began laboratory radiation studies in 1980 and found that rats exposed to radiofrequency radiation had damaged brain DNA. He maintains a database that holds 400 scientific papers on possible biological effects of radiation from wireless communication. He found that 28 percent of studies with cellphone industry funding showed some sort of effect, while 67 percent of studies without such funding did so.

The unit of measurement for radiofrequency exposure is called the specific absorption rate, or SAR. The Federal Communications Commission mandates that the SAR produced by phones be no more than 1.6 watts per kilogram. One study listed by Mr. Lai found effects like loss of memory in rats exposed to SAR values in the range of 0.0006 to 0.06 watts per kilogram. "I did not expect to see effects at low levels," he said.

The 737 minutes that we talk on cellphones monthly, on average, according to the C.T.I.A., makes today's typical user indistinguishable from the heavy user of 10 years ago. Ms. Davis recommends keeping a phone out of close proximity to the head or body, by using wired headsets or the phone's speaker. Children should text rather than call, she said, and pregnant women should keep phones away from the abdomen. The F.C.C. concurs about the best way to avoid exposure. It is not by choosing a phone with a marginally lower SAR, it says, but rather by holding the cellphone "away from the head or body."

Summary

- Employers search social networking sites, such as Facebook or Instagram, to find background information on applicants
- Spamming presents serious privacy issues
- Two types of information available on the Web are public and private
- Many associations promote the ethically responsible use of information systems and technologies
- Information technology has created many new jobs
- Green computing is one of the methods for combating global warming

Library and Web References

- Contemporary Issues in Ethics and Information Technology,
<http://ezproxy.cbu.edu:9000/login?url=http://www.netlibrary.com/urlapi.asp?action=summary&v=1&bookid=140156>
- [Privacy Crisis: Identity Theft Prevention Plan and Guide to Anonymous Living](#) by Grant Hall
- [Privacy Protection and Computer Forensics, Second Edition](#) by Michael A. Caloyannides
- [Internet Privacy for Dummies](#) by John R. Levine, Ray Everett-Church, Gregg Stebben, and David Lawrence
- [Technology and Privacy: The New Landscape](#) by Philip E. Agre and Marc Rotenberg

Homework

- Textbook Chapter Four
- Quiz on these chapters
- Individually for ABC email:
 - Key (**operational/strategic not supportive**) business process definitions
 - Information needs – Partial information model (Entities and identifiers in Access) only at this point (relationships due later) – take screen copy of Access relationship window -**see next slide for example with relationships**
- **Team Report 2**
 - Competitive Analysis
 - Critical Success Factors
 - Strategic Use of Information Technology

This is a screen shot of the Access relationship grid and shows a full information model; **the partial model only includes the entities and entity identifiers** (shown as Access keys here), not the attributes (Access columns) and relationships

