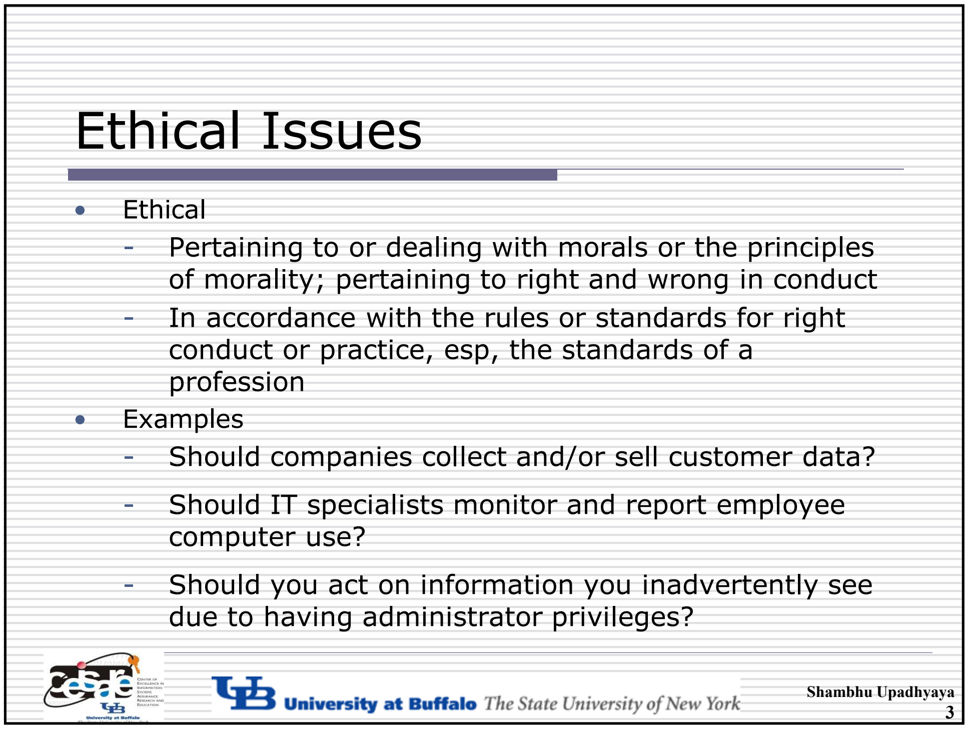
Legal and Ethical Issues in Computer Security

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 25)

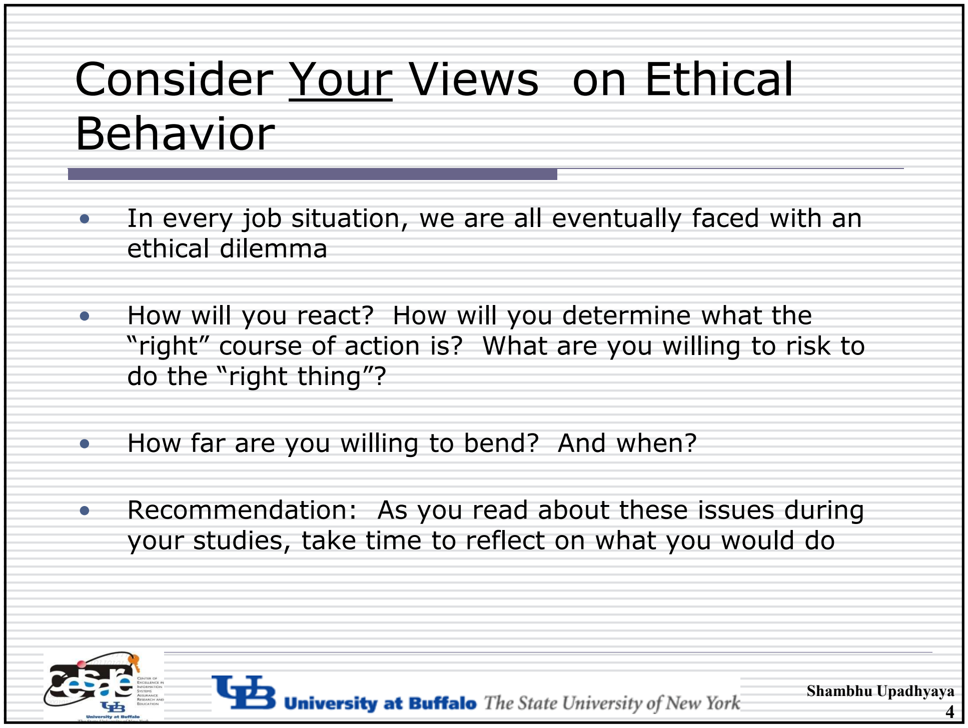
Ethical vs. Legal Issues

- Legal issues
  - Sometimes have a definitive answer
  - Determination is made by others (not you)
- Ethical issues
  - Sometimes have a definitive answer
  - You determine your course of action
- The law doesn’t make it “right”
- Being “right” doesn’t make it legal



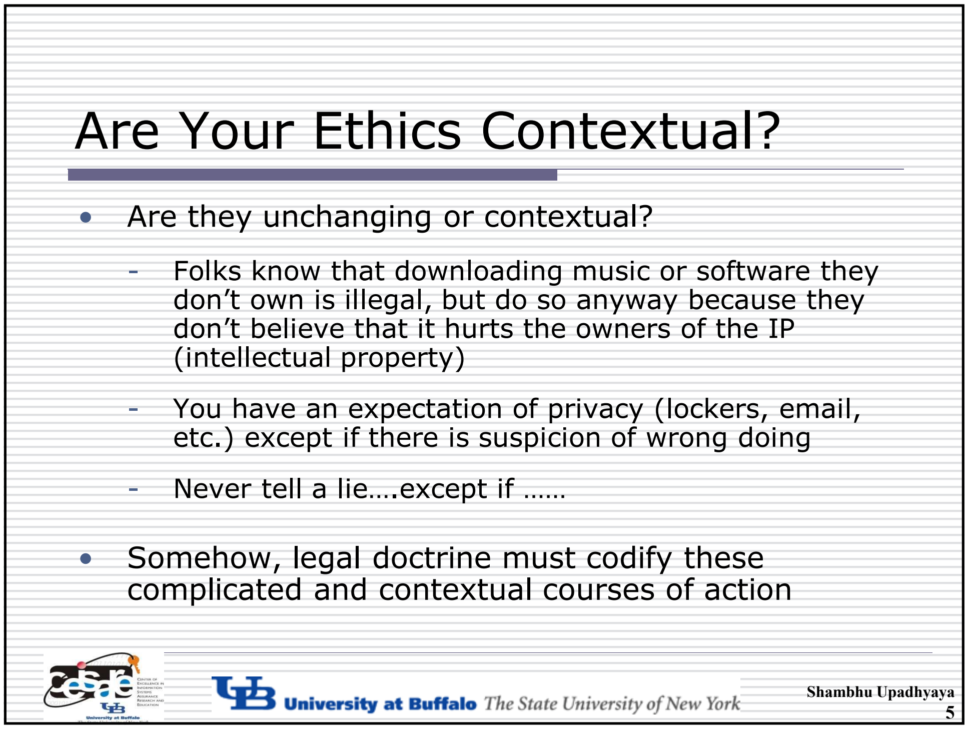
Ethical Issues

- Ethical
  - Pertaining to or dealing with morals or the principles of morality; pertaining to right and wrong in conduct
  - In accordance with the rules or standards for right conduct or practice, esp, the standards of a profession
- Examples
  - Should companies collect and/or sell customer data?
  - Should IT specialists monitor and report employee computer use?
  - Should you act on information you inadvertently see due to having administrator privileges?



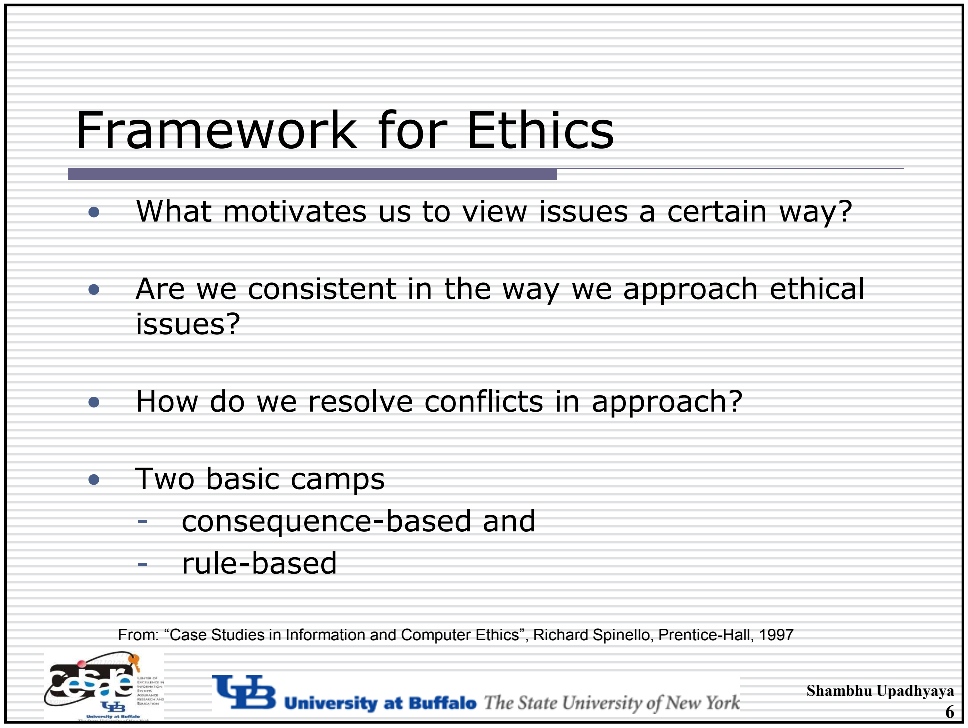
Consider Your Views on Ethical Behavior

- In every job situation, we are all eventually faced with an ethical dilemma
- How will you react? How will you determine what the “right” course of action is? What are you willing to risk to do the “right thing”?
- How far are you willing to bend? And when?
- Recommendation: As you read about these issues during your studies, take time to reflect on what you would do



Are Your Ethics Contextual?

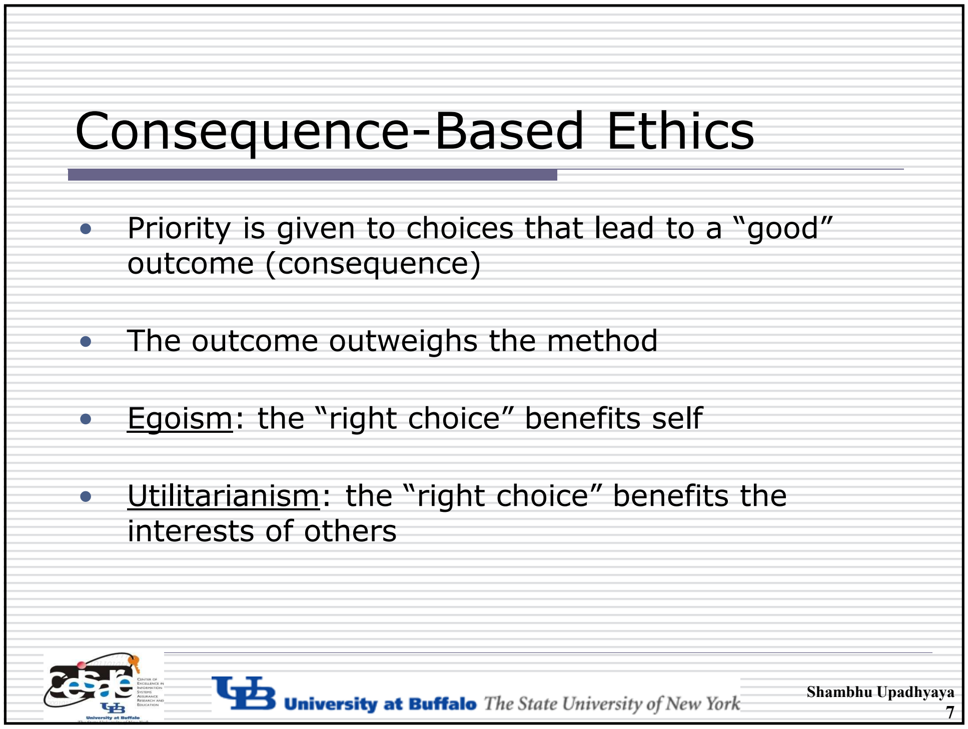
- Are they unchanging or contextual?
  - Folks know that downloading music or software they don’t own is illegal, but do so anyway because they don’t believe that it hurts the owners of the IP (intellectual property)
  - You have an expectation of privacy (lockers, email, etc.) except if there is suspicion of wrong doing
  - Never tell a lie….except if ……
- Somehow, legal doctrine must codify these complicated and contextual courses of action



Framework for Ethics

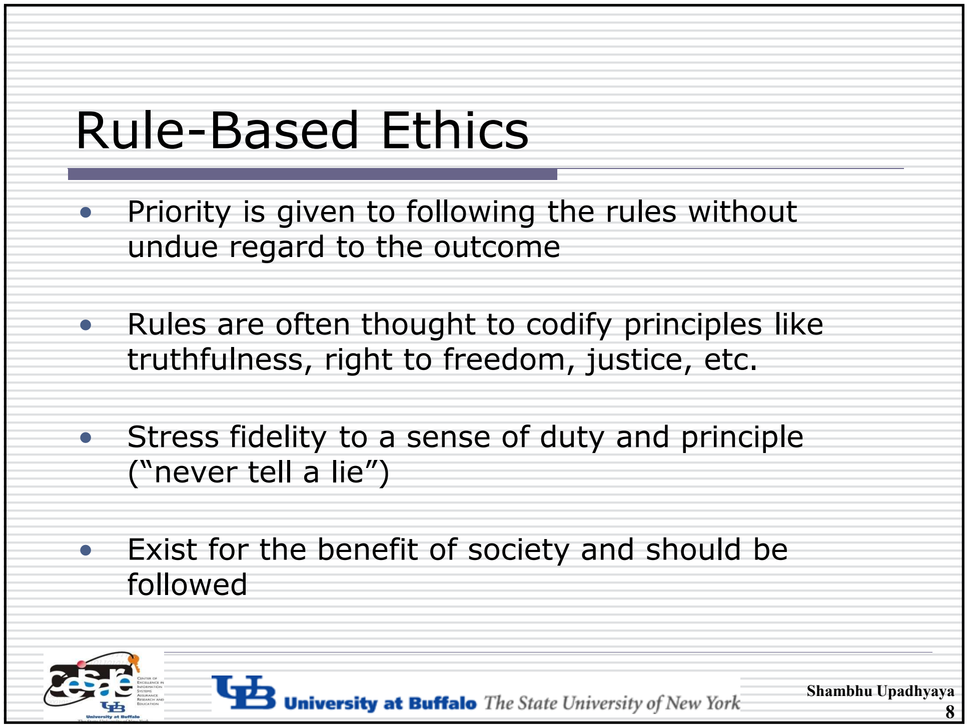
- What motivates us to view issues a certain way?
- Are we consistent in the way we approach ethical issues?
- How do we resolve conflicts in approach?
- Two basic camps
  - consequence-based and
  - rule-based

From: “Case Studies in Information and Computer Ethics”, Richard Spinello, Prentice-Hall, 1997



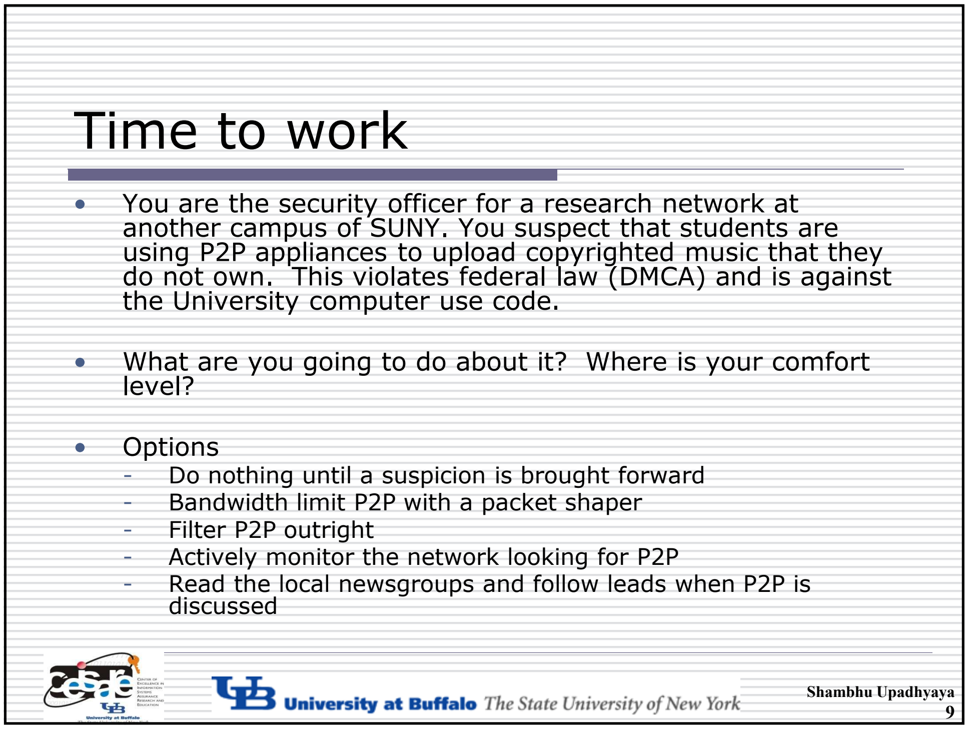
Consequence-Based Ethics

- Priority is given to choices that lead to a “good” outcome (consequence)
- The outcome outweighs the method
- Egoism: the “right choice” benefits self
- Utilitarianism: the “right choice” benefits the interests of others



Rule-Based Ethics

- Priority is given to following the rules without undue regard to the outcome
- Rules are often thought to codify principles like truthfulness, right to freedom, justice, etc.
- Stress fidelity to a sense of duty and principle (“never tell a lie”)
- Exist for the benefit of society and should be followed

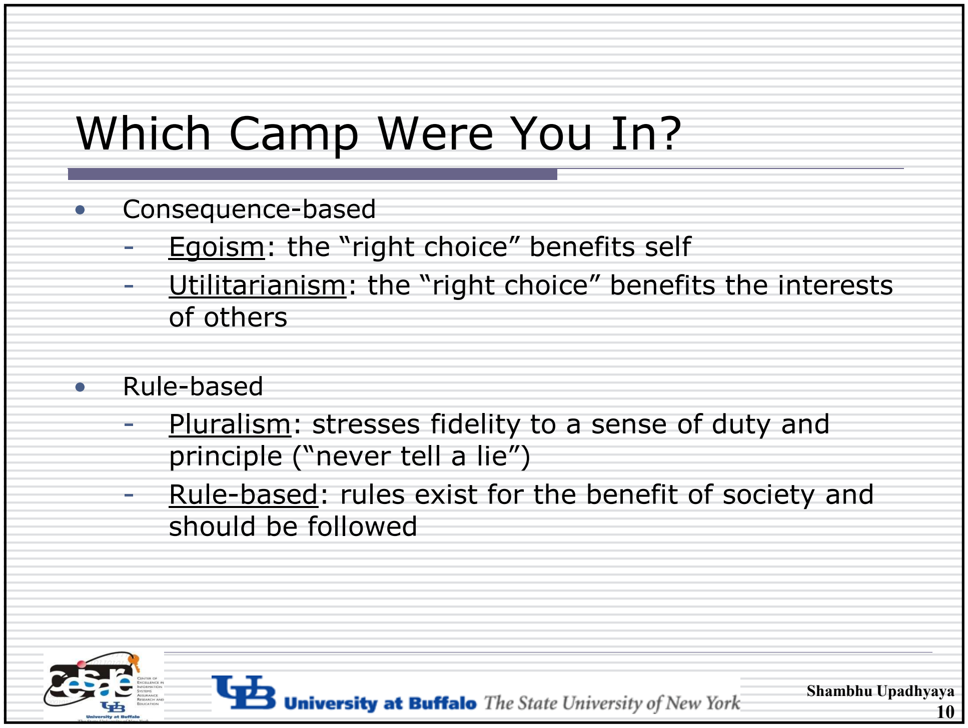


Time to work

- You are the security officer for a research network at another campus of SUNY. You suspect that students are using P2P appliances to upload copyrighted music that they do not own. This violates federal law (DMCA) and is against the University computer use code.

- What are you going to do about it? Where is your comfort level?

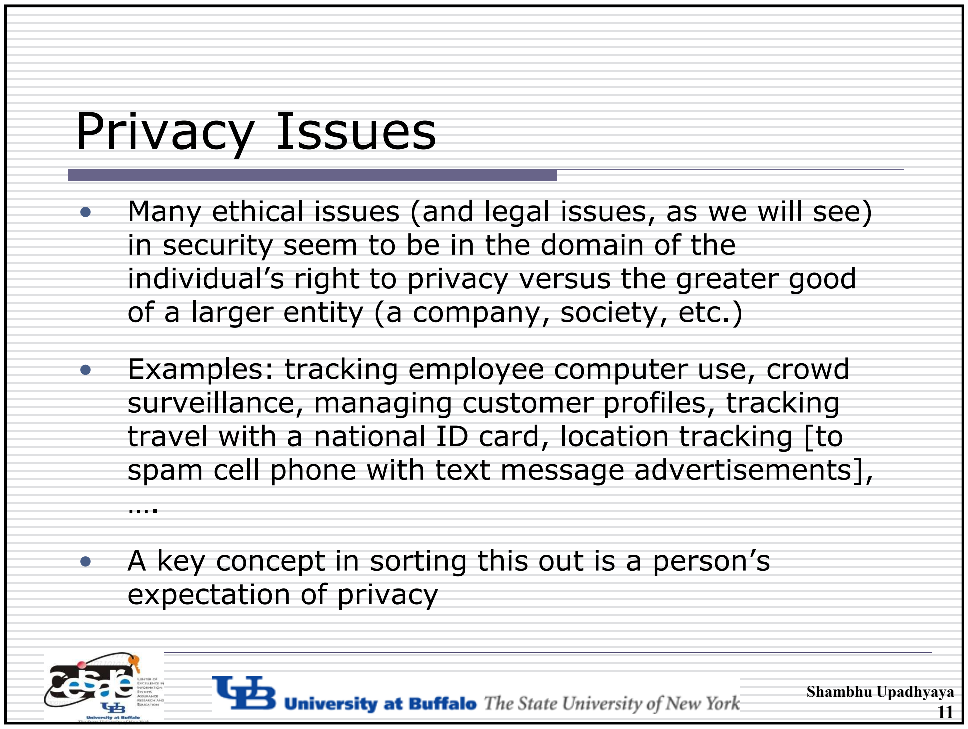
- Options
  - Do nothing until a suspicion is brought forward
  - Bandwidth limit P2P with a packet shaper
  - Filter P2P outright
  - Actively monitor the network looking for P2P
  - Read the local newsgroups and follow leads when P2P is discussed



Which Camp Were You In?

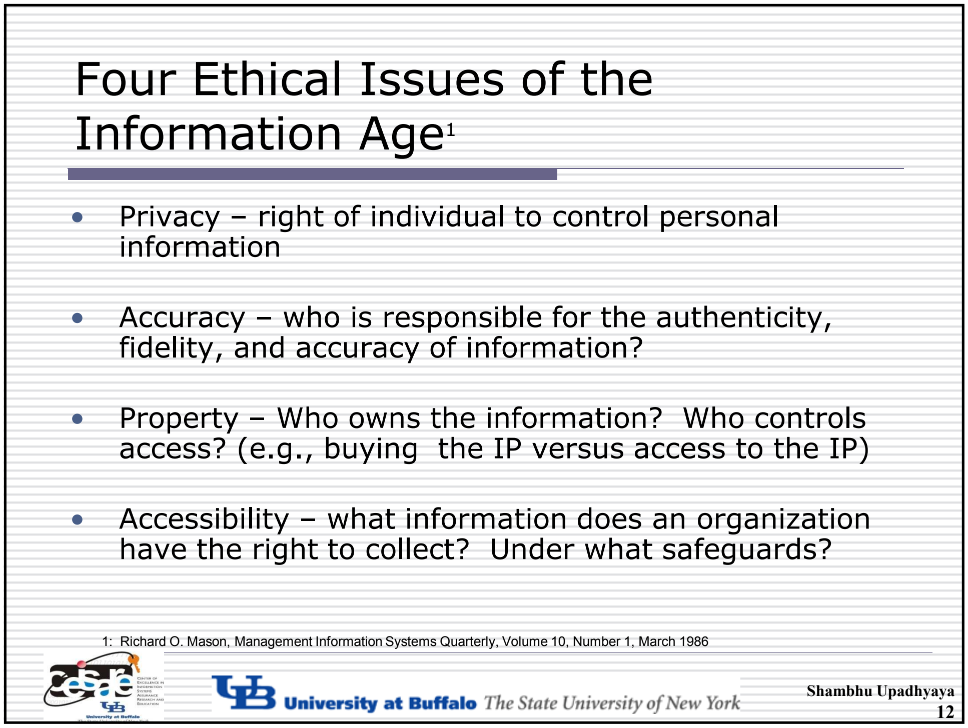
- Consequence-based
  - Egoism: the “right choice” benefits self
  - Utilitarianism: the “right choice” benefits the interests of others

- Rule-based
  - Pluralism: stresses fidelity to a sense of duty and principle (“never tell a lie”)
  - Rule-based: rules exist for the benefit of society and should be followed



Privacy Issues

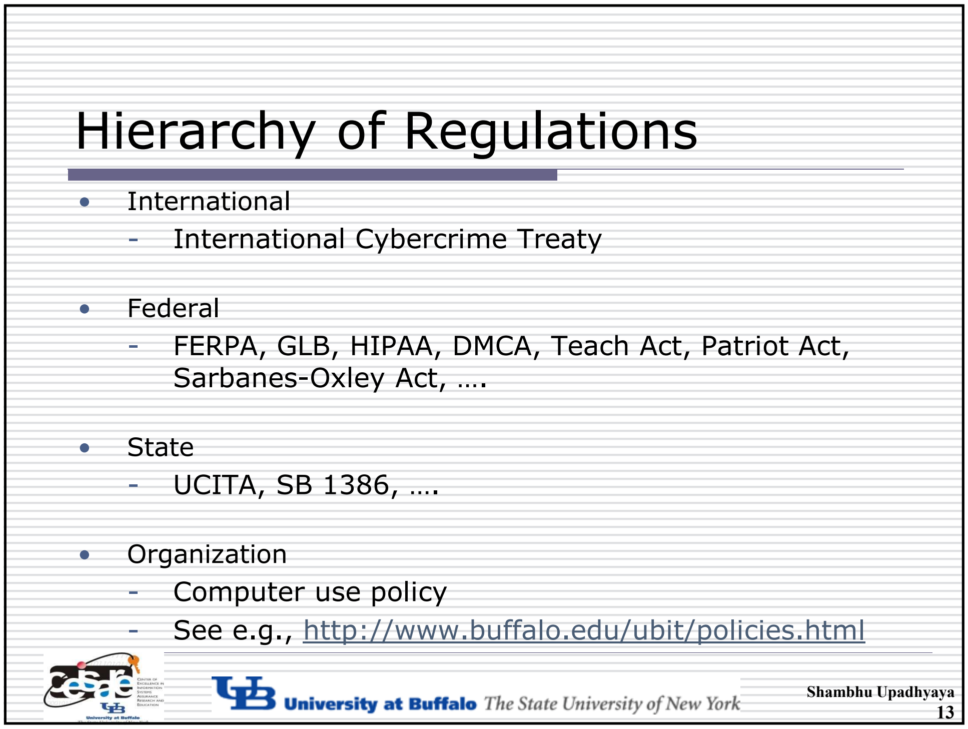
- Many ethical issues (and legal issues, as we will see) in security seem to be in the domain of the individual’s right to privacy versus the greater good of a larger entity (a company, society, etc.)
- Examples: tracking employee computer use, crowd surveillance, managing customer profiles, tracking travel with a national ID card, location tracking [to spam cell phone with text message advertisements], ….
- A key concept in sorting this out is a person’s expectation of privacy



Four Ethical Issues of the Information Age[1]

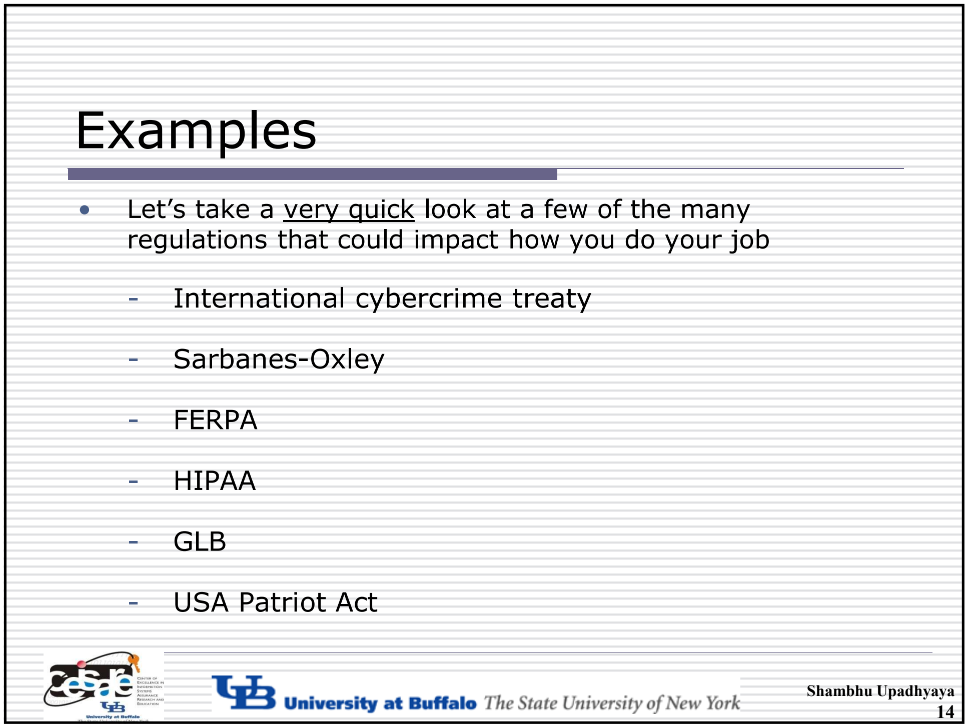
- Privacy – right of individual to control personal information
- Accuracy – who is responsible for the authenticity, fidelity, and accuracy of information?
- Property – Who owns the information? Who controls access? (e.g., buying the IP versus access to the IP)
- Accessibility – what information does an organization have the right to collect? Under what safeguards?

[1] Richard O. Mason, Management Information Systems Quarterly, Volume 10, Number 1, March 1986



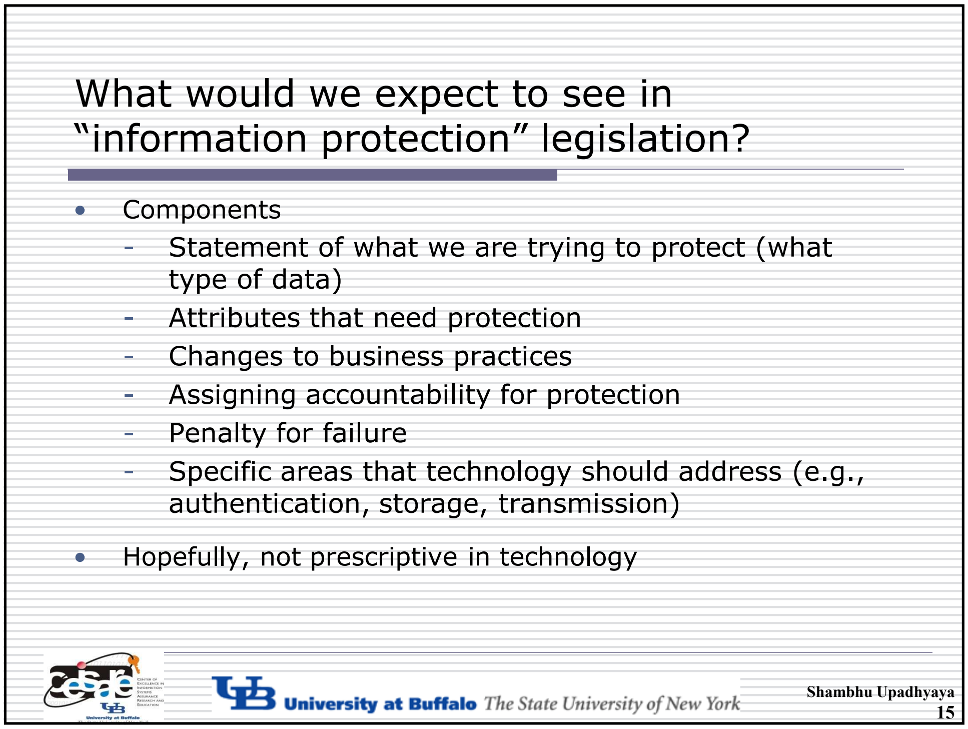
Hierarchy of Regulations

- International
  - International Cybercrime Treaty
- Federal
  - FERPA, GLB, HIPAA, DMCA, Teach Act, Patriot Act, Sarbanes-Oxley Act, ….
- State
  - UCITA, SB 1386, ….
- Organization
  - Computer use policy
  - See e.g., http://www.buffalo.edu/ubit/policies.html



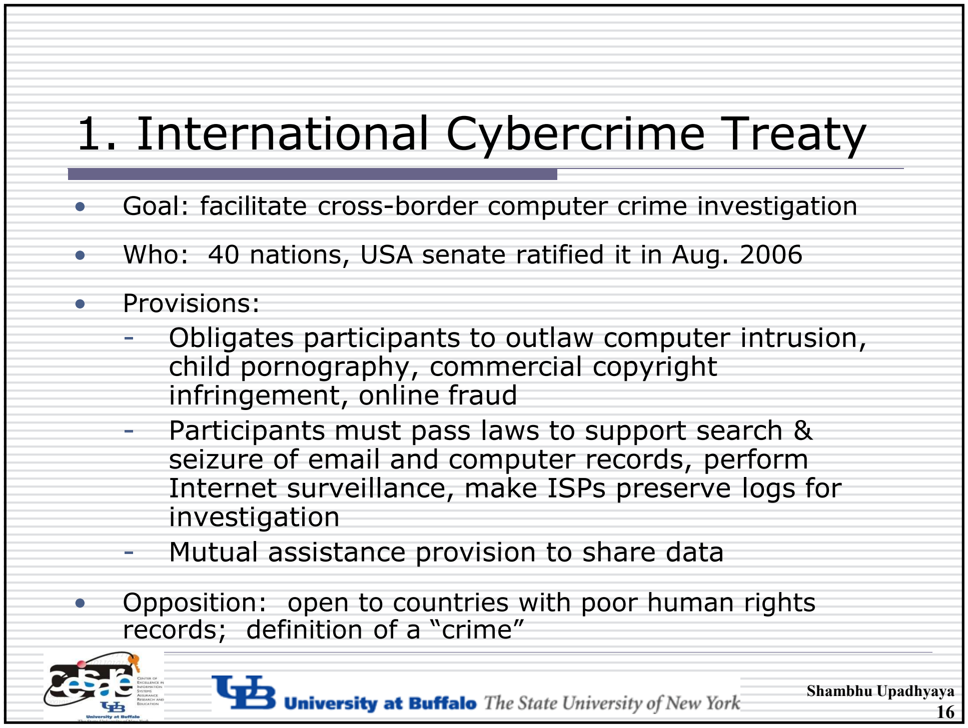
Examples

- Let's take a very quick look at a few of the many regulations that could impact how you do your job
  - International cybercrime treaty
  - Sarbanes-Oxley
  - FERPA
  - HIPAA
  - GLB
  - USA Patriot Act



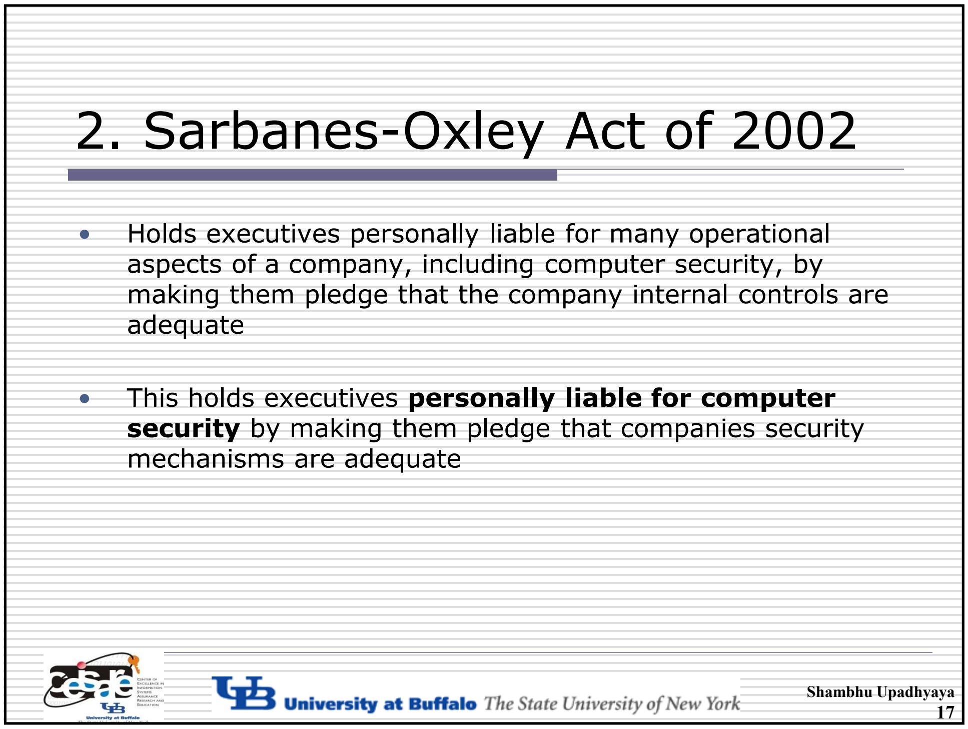
What would we expect to see in "information protection" legislation?

- Components
  - Statement of what we are trying to protect (what type of data)
  - Attributes that need protection
  - Changes to business practices
  - Assigning accountability for protection
  - Penalty for failure
  - Specific areas that technology should address (e.g., authentication, storage, transmission)
- Hopefully, not prescriptive in technology



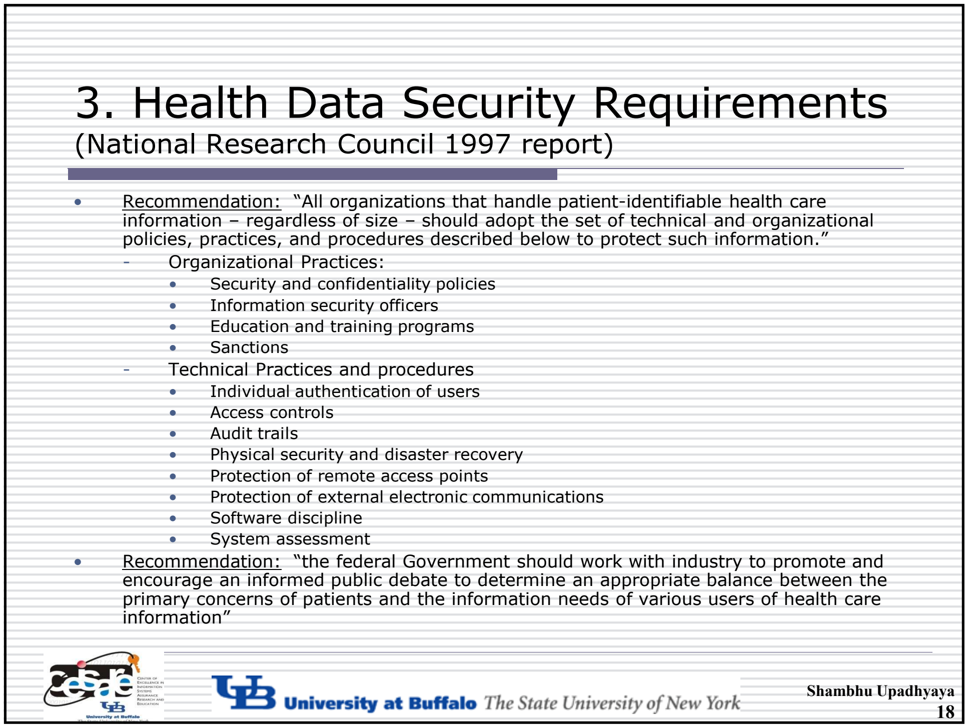
1. International Cybercrime Treaty

- Goal: facilitate cross-border computer crime investigation
- Who: 40 nations, USA senate ratified it in Aug. 2006
- Provisions:
  - Obligates participants to outlaw computer intrusion, child pornography, commercial copyright infringement, online fraud
  - Participants must pass laws to support search & seizure of email and computer records, perform Internet surveillance, make ISPs preserve logs for investigation
  - Mutual assistance provision to share data
- Opposition: open to countries with poor human rights records; definition of a "crime"



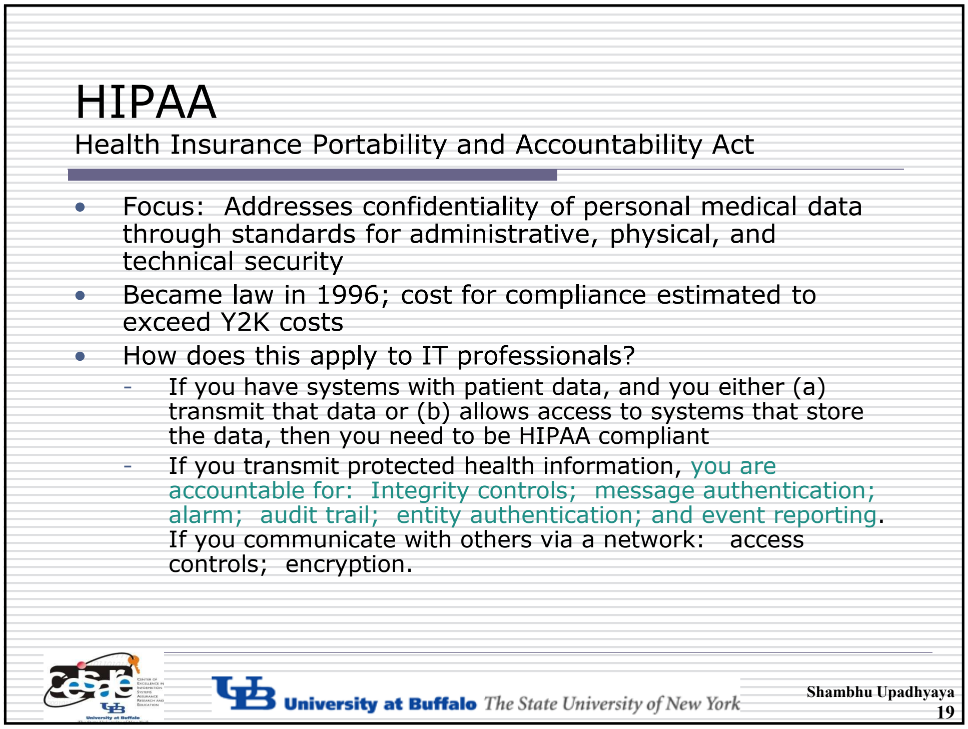
2. Sarbanes-Oxley Act of 2002

- Holds executives personally liable for many operational aspects of a company, including computer security, by making them pledge that the company internal controls are adequate
- This holds executives **personally liable for computer security** by making them pledge that companies security mechanisms are adequate



3. Health Data Security Requirements
(National Research Council 1997 report)

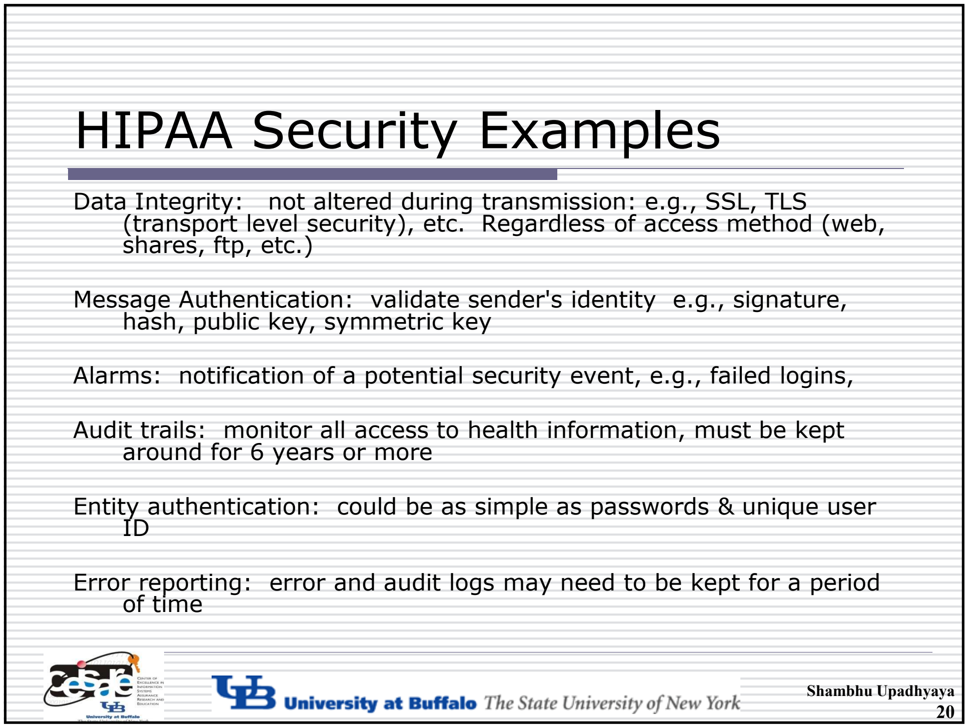
- Recommendation: "All organizations that handle patient-identifiable health care information – regardless of size – should adopt the set of technical and organizational policies, practices, and procedures described below to protect such information."
  - Organizational Practices:
    - Security and confidentiality policies
    - Information security officers
    - Education and training programs
    - Sanctions
  - Technical Practices and procedures
    - Individual authentication of users
    - Access controls
    - Audit trails
    - Physical security and disaster recovery
    - Protection of remote access points
    - Protection of external electronic communications
    - Software discipline
    - System assessment
- Recommendation: "the federal Government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the primary concerns of patients and the information needs of various users of health care information"



HIPAA

Health Insurance Portability and Accountability Act

- Focus: Addresses confidentiality of personal medical data through standards for administrative, physical, and technical security
- Became law in 1996; cost for compliance estimated to exceed Y2K costs
- How does this apply to IT professionals?
  - If you have systems with patient data, and you either (a) transmit that data or (b) allows access to systems that store the data, then you need to be HIPAA compliant
  - If you transmit protected health information, you are accountable for: Integrity controls; message authentication; alarm; audit trail; entity authentication; and event reporting. If you communicate with others via a network: access controls; encryption.



HIPAA Security Examples

Data Integrity: not altered during transmission: e.g., SSL, TLS (transport level security), etc. Regardless of access method (web, shares, ftp, etc.)

Message Authentication: validate sender's identity e.g., signature, hash, public key, symmetric key

Alarms: notification of a potential security event, e.g., failed logins,

Audit trails: monitor all access to health information, must be kept around for 6 years or more

Entity authentication: could be as simple as passwords & unique user ID

Error reporting: error and audit logs may need to be kept for a period of time

HIPAA Security Areas

1. Administrative procedures to guard data CIA. Documented formal procedures to select and measure security mechanisms

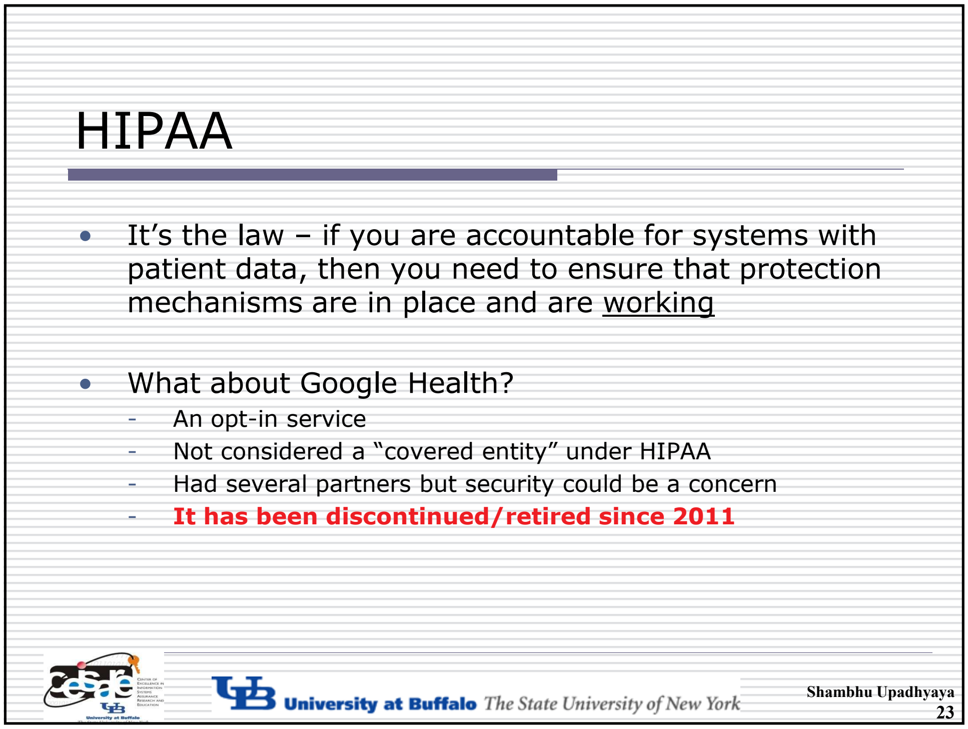
2. Physical safeguards to protect computers, buildings, data

3. Technical security services, including processes to protect information

4. Technical security mechanisms to prevent unauthorized access to stored or transmitted data

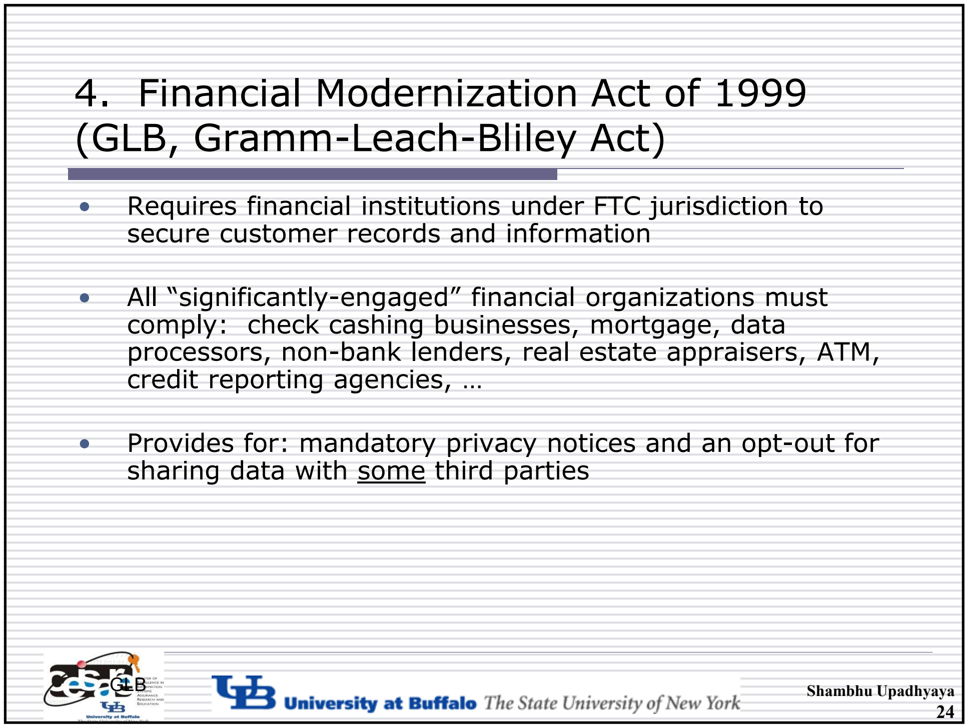
Appendix A – Security Safeguards

- Administrative Safeguards
  - Security management processes: risk analysis, risk management, sanction policy, information systems activity review
  - Assigned security responsibility: identified person accountable for security
  - Workforce security: processes for clearance, authorization, and termination
  - Incident procedures: response and reporting
  - Contingency plan: backup, disaster recovery, testing
- Physical Safeguards
  - Facility Access controls: contingency operations, facility security plan
  - Workstation use:
  - Workstation security:
  - Device and media controls: disposal, media re-use, backup
- Technical safeguards:
  - Access control: unique user ids, automatic logoff, encryption, emergency access
  - Audit controls: required
  - Integrity: mechanism to authenticate electronic protected health information
  - Entity authentication: required
  - Transmission security: integrity controls., encryption



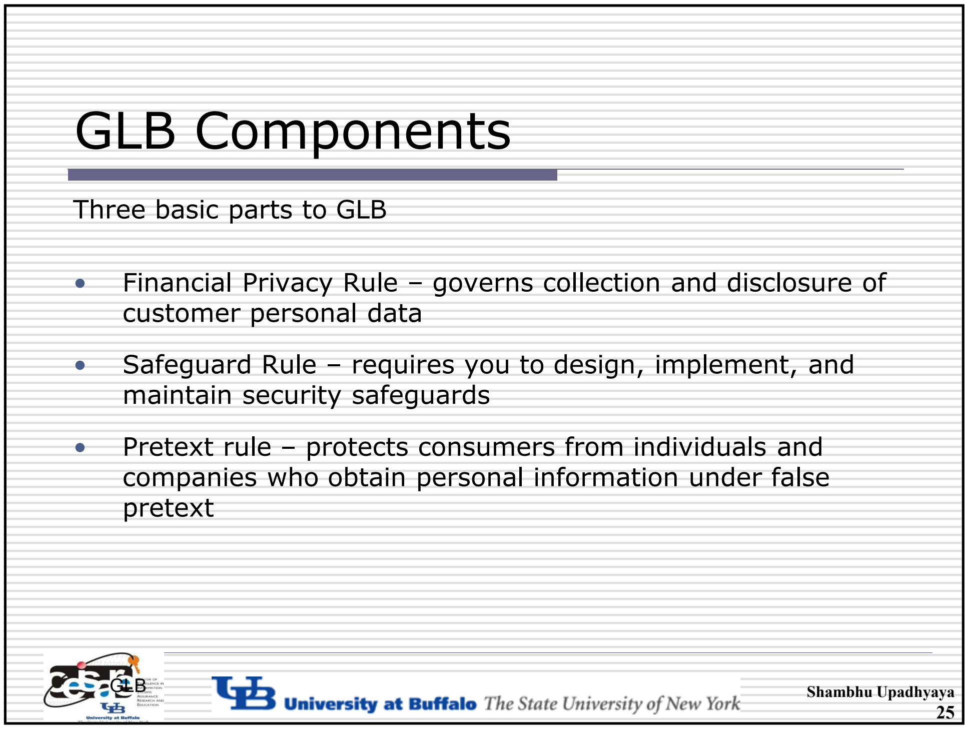
HIPAA

- It’s the law – if you are accountable for systems with patient data, then you need to ensure that protection mechanisms are in place and are <u>working</u>
- What about Google Health?
  - An opt-in service
  - Not considered a “covered entity” under HIPAA
  - Had several partners but security could be a concern
  - **It has been discontinued/retired since 2011**



4. Financial Modernization Act of 1999 (GLB, Gramm-Leach-Bliley Act)

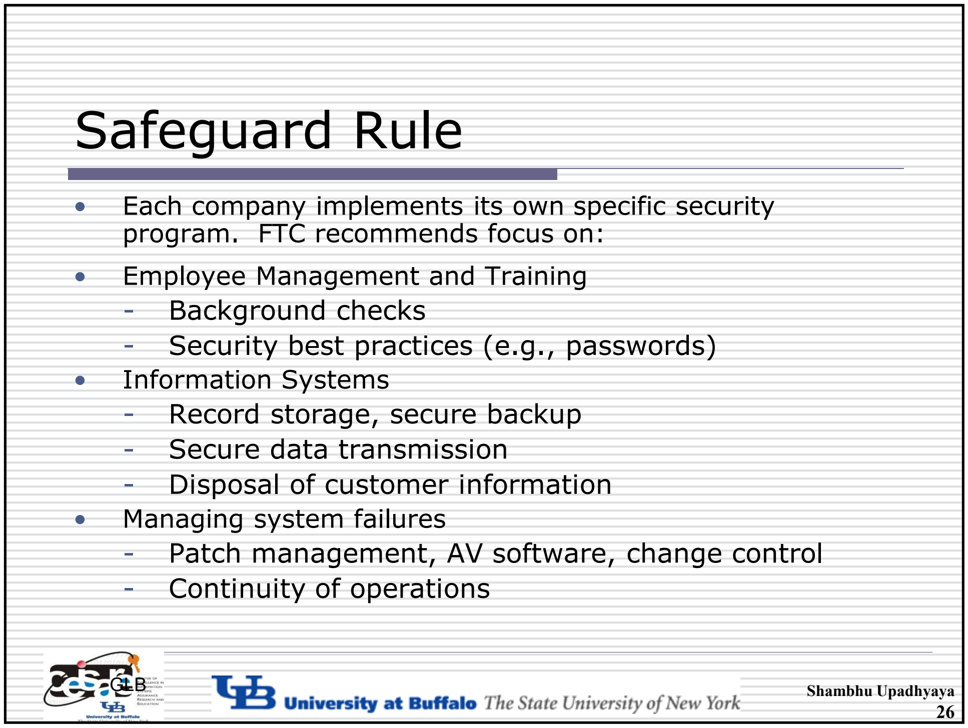
- Requires financial institutions under FTC jurisdiction to secure customer records and information
- All “significantly-engaged” financial organizations must comply: check cashing businesses, mortgage, data processors, non-bank lenders, real estate appraisers, ATM, credit reporting agencies, …
- Provides for: mandatory privacy notices and an opt-out for sharing data with <u>some</u> third parties



GLB Components

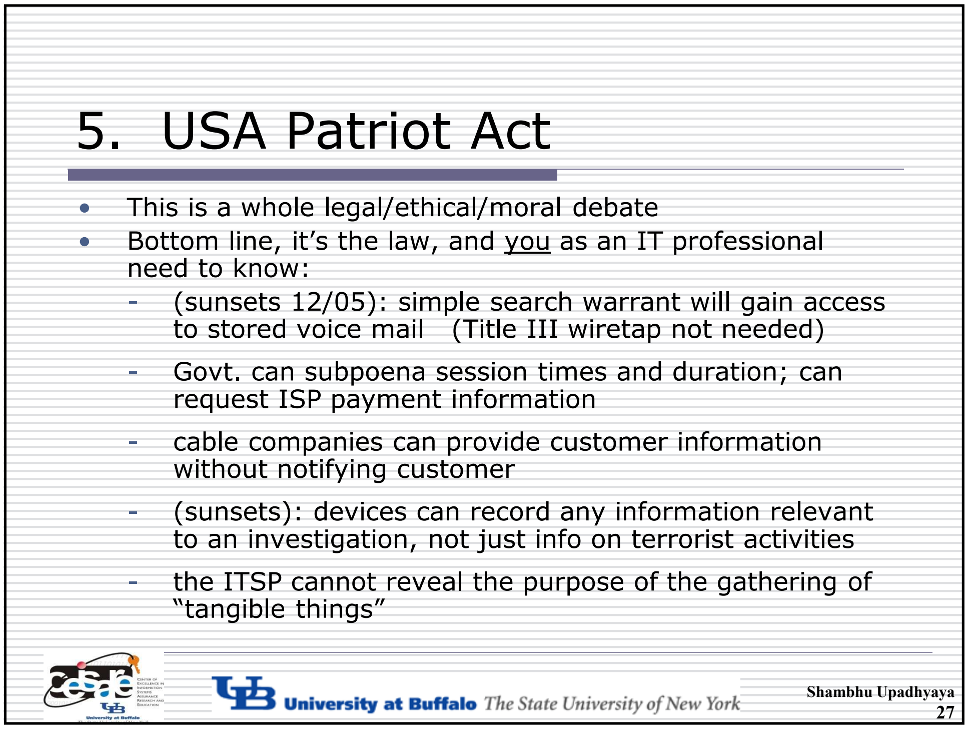
Three basic parts to GLB

- Financial Privacy Rule – governs collection and disclosure of customer personal data
- Safeguard Rule – requires you to design, implement, and maintain security safeguards
- Pretext rule – protects consumers from individuals and companies who obtain personal information under false pretext



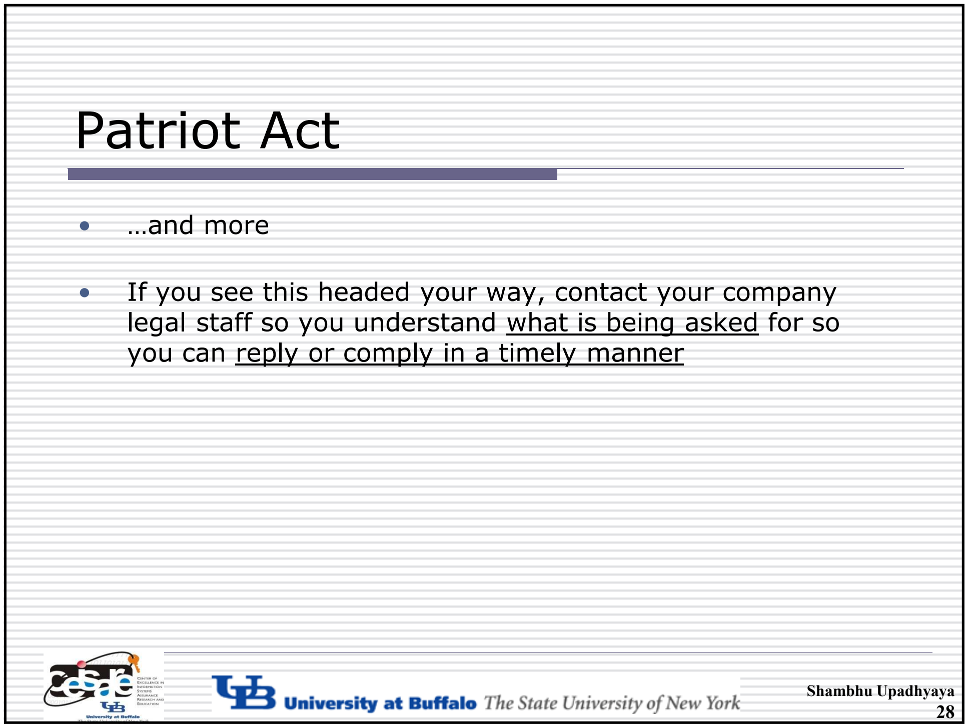
Safeguard Rule

- Each company implements its own specific security program. FTC recommends focus on:
- Employee Management and Training
  - Background checks
  - Security best practices (e.g., passwords)
- Information Systems
  - Record storage, secure backup
  - Secure data transmission
  - Disposal of customer information
- Managing system failures
  - Patch management, AV software, change control
  - Continuity of operations



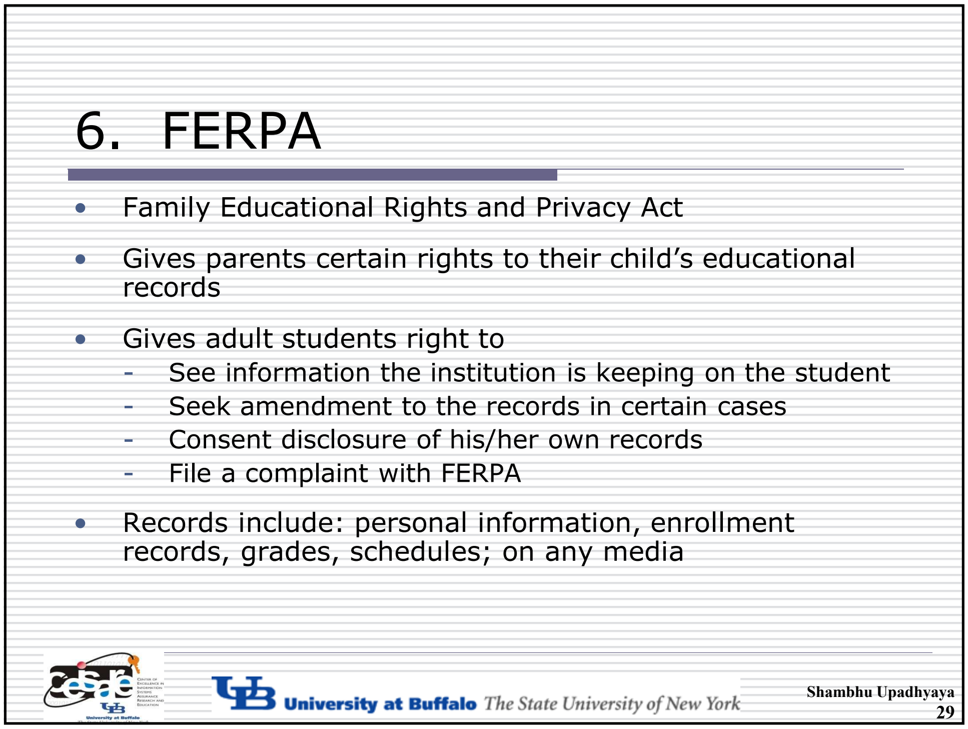
5. USA Patriot Act

- This is a whole legal/ethical/moral debate
- Bottom line, it’s the law, and <u>you</u> as an IT professional need to know:
  - (sunsets 12/05): simple search warrant will gain access to stored voice mail (Title III wiretap not needed)
  - Govt. can subpoena session times and duration; can request ISP payment information
  - cable companies can provide customer information without notifying customer
  - (sunsets): devices can record any information relevant to an investigation, not just info on terrorist activities
  - the ITSP cannot reveal the purpose of the gathering of “tangible things”



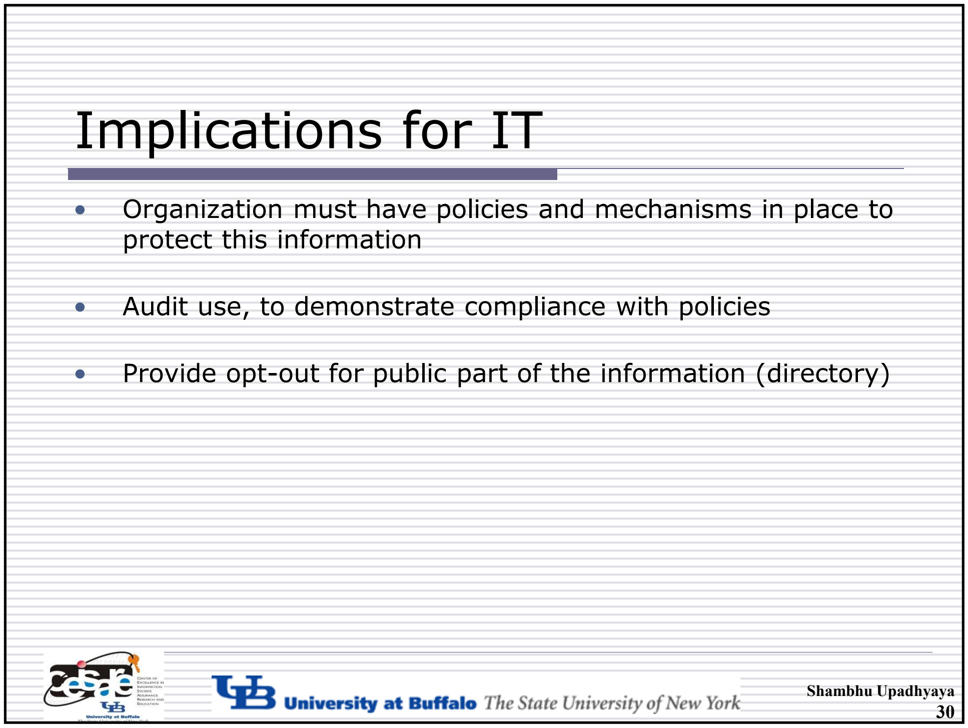
Patriot Act

- …and more
- If you see this headed your way, contact your company legal staff so you understand <u>what is being asked</u> for so you can <u>reply or comply in a timely manner</u>



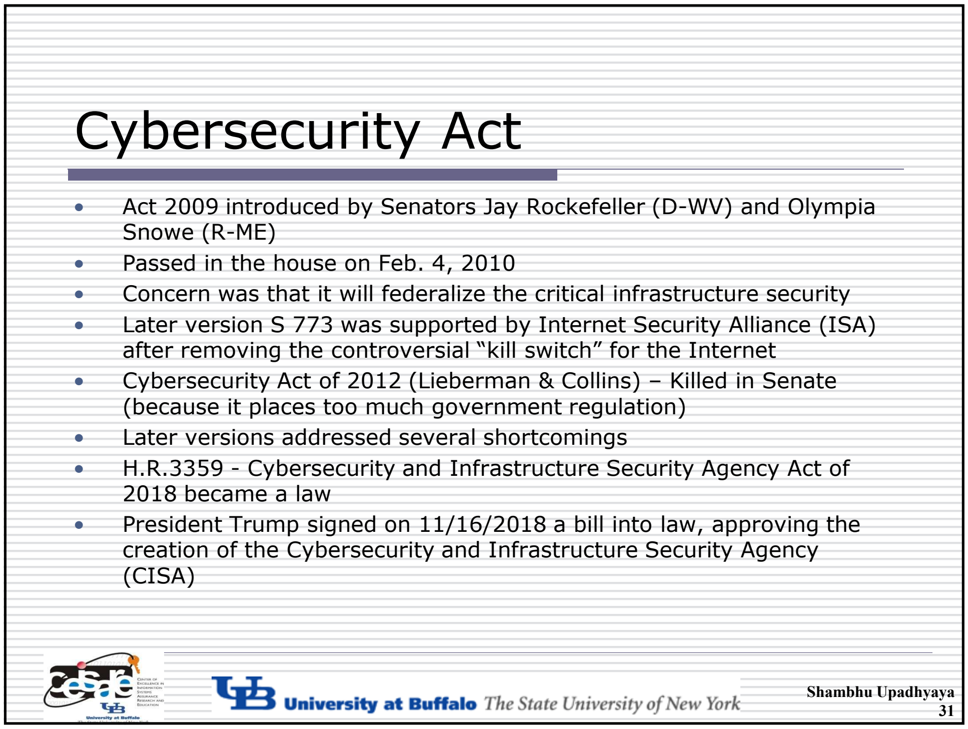
6. FERPA

- Family Educational Rights and Privacy Act
- Gives parents certain rights to their child’s educational records
- Gives adult students right to
  - See information the institution is keeping on the student
  - Seek amendment to the records in certain cases
  - Consent disclosure of his/her own records
  - File a complaint with FERPA
- Records include: personal information, enrollment records, grades, schedules; on any media



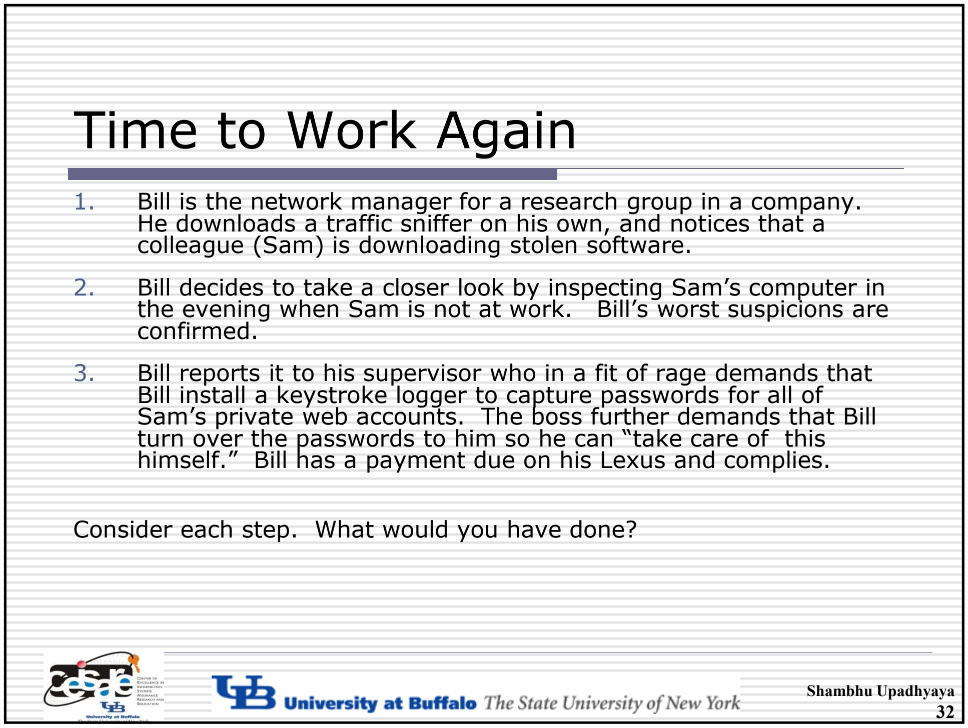
Implications for IT

- Organization must have policies and mechanisms in place to protect this information
- Audit use, to demonstrate compliance with policies
- Provide opt-out for public part of the information (directory)



Cybersecurity Act

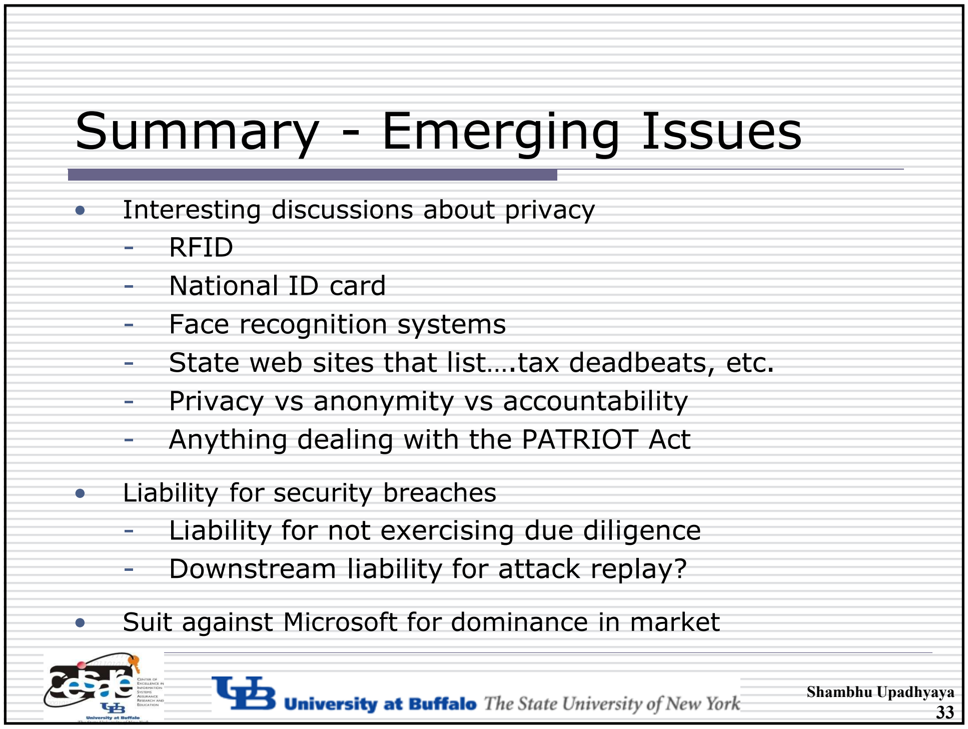
- Act 2009 introduced by Senators Jay Rockefeller (D-WV) and Olympia Snowe (R-ME)
- Passed in the house on Feb. 4, 2010
- Concern was that it will federalize the critical infrastructure security
- Later version S 773 was supported by Internet Security Alliance (ISA) after removing the controversial "kill switch" for the Internet
- Cybersecurity Act of 2012 (Lieberman & Collins) – Killed in Senate (because it places too much government regulation)
- Later versions addressed several shortcomings
- H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018 became a law
- President Trump signed on 11/16/2018 a bill into law, approving the creation of the Cybersecurity and Infrastructure Security Agency (CISA)



Time to Work Again

1. Bill is the network manager for a research group in a company. He downloads a traffic sniffer on his own, and notices that a colleague (Sam) is downloading stolen software.
2. Bill decides to take a closer look by inspecting Sam's computer in the evening when Sam is not at work. Bill's worst suspicions are confirmed.
3. Bill reports it to his supervisor who in a fit of rage demands that Bill install a keystroke logger to capture passwords for all of Sam's private web accounts. The boss further demands that Bill turn over the passwords to him so he can "take care of this himself." Bill has a payment due on his Lexus and complies.

Consider each step. What would you have done?

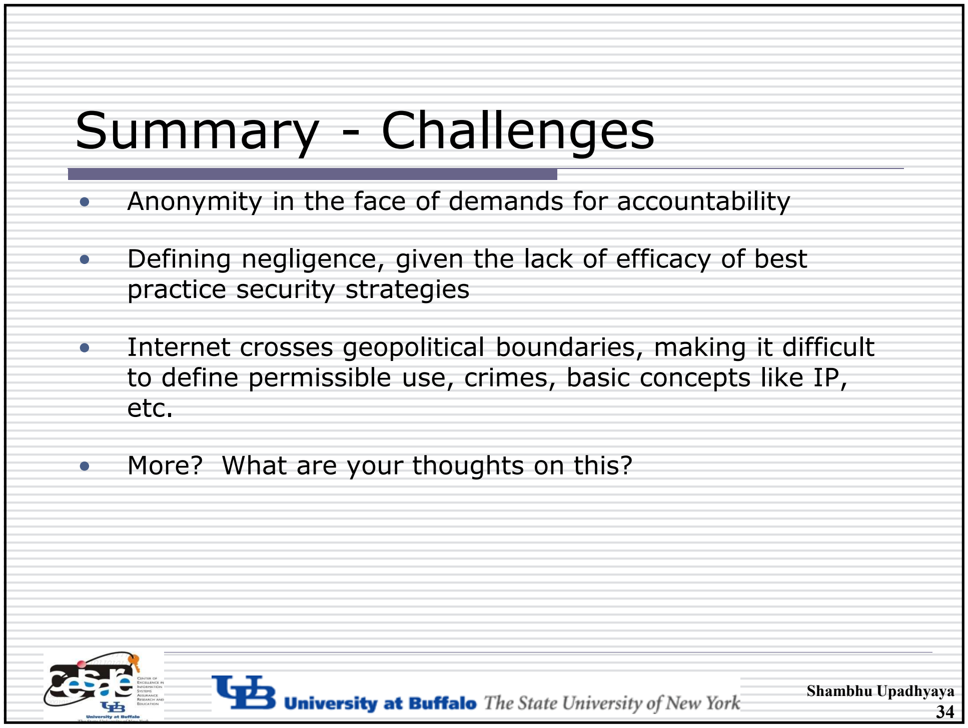


Summary - Emerging Issues

- Interesting discussions about privacy
  - RFID
  - National ID card
  - Face recognition systems
  - State web sites that list….tax deadbeats, etc.
  - Privacy vs anonymity vs accountability
  - Anything dealing with the PATRIOT Act
- Liability for security breaches
  - Liability for not exercising due diligence
  - Downstream liability for attack replay?
- Suit against Microsoft for dominance in market

University at Buffalo The State University of New York

Shambhu Upadhyaya
33

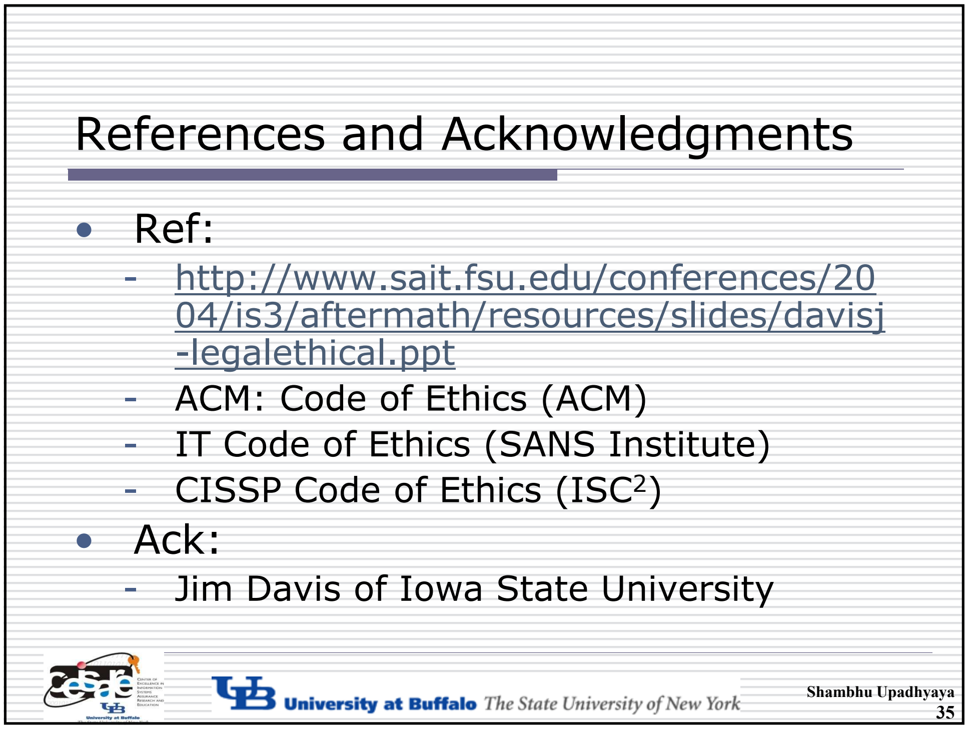


Summary - Challenges

- Anonymity in the face of demands for accountability
- Defining negligence, given the lack of efficacy of best practice security strategies
- Internet crosses geopolitical boundaries, making it difficult to define permissible use, crimes, basic concepts like IP, etc.
- More? What are your thoughts on this?

University at Buffalo The State University of New York

Shambhu Upadhyaya
34



References and Acknowledgments

- Ref:
  - http://www.sait.fsu.edu/conferences/2004/is3/aftermath/resources/slides/davisj-legalethical.ppt
  - ACM: Code of Ethics (ACM)
  - IT Code of Ethics (SANS Institute)
  - CISSP Code of Ethics (ISC^2)
- Ack:
  - Jim Davis of Iowa State University