**Unit 1: Reasons to Regulate Internet Services and Networks**

***Vocabulary***

* Pareto efficiency: reallocating resources so that it’s impossible for one individual to be better off than the other
* Public Choice Theory: assuming government actors maximize their own private goals
* Wise Man Theory: (of regulation) establishes command-and-control organization, only the regulator knows what is best for the public

***Key Concept Questions***

* Why should we care about Internet and telecommunications policies?
* What are the reasons for regulation in the Internet and telecommunications sectors?
* What are the steps to apply the interdisciplinary telecom framework to recommend new or revised policies or regulations?
* Should there be any difference in how the Internet is regulated compared to traditional telecommunications regulatory models?

***Terms and Concepts***

*Interdisciplinary Policy Framework*

* (1)Identify Problem and Current Policy
  + Describe the nature and extent of the problem with clear evidence
  + Identify key players and affected populations
  + Establish drivers and underlying causes
  + Develop status quo (current policies, what will happen without new policy action)
* (2) Define Policy Objectives
  + Describe objectives that correspond to main problem and its root causes that justify regulation
  + Establish objectives at number of levels, going from general to specific/operational
  + Evaluate objectives using SMART terms
    - **S**pecific
    - **M**easurable
    - **A**chievable
    - **R**ealistic
    - **T**ime-Dependent
* (3) Role of Technology
  + Identify technology creating the problem
  + Identifying key technologies at number of levels, going from systematic to specific/operational
  + Maintain narrow range of technical focus
* (4) Develop Policy Options for Analysis
  + Identify policy options that vary due to major variations in significant attributes linked to policy objectives
    - Always include status quo option of existing policy
  + Identify important technical, economic and social factors that reveal substantial and important differences in evaluation of efficacy of policy options
  + Using Factors to Evaluate Options
    - (1) Identify key technical, economic and social impacts
    - (2) Qualitative assessment of largest impacts
    - (3) In-depth qualitative/quantitative analysis of largest impacts
* (5) Compare and Analyze Options
  + Clearly support prioritization of factors
  + Resulting analysis should clearly identify who or what is affected and in what way by each of the factors
  + Compare and present positive and negative impacts overall for each option based upon factors (cost benefit analysis)
  + Consider risks and uncertainties in policy choices
  + Identify preferred option

*Reasons for Public Intervention*

* Market Failures
  + Weak competition (abuse of market power) due to natural monopoly or network effects
  + Market prices do not reflect real costs and benefits to society (negative externalities)
  + Insufficient supply of public goods
  + Missing or incomplete markets
  + Information failures, such as imperfect information or lack of access to information for decision takes (including consumers and public authorities)
* Regulatory Failures
  + Inadequately defined property rights/legal framework
  + Poorly defined targets and objectives
  + Unintended consequences resulting from public intervention
  + Regulatory capture of public authorities
  + Implementation and enforcement failures
* Market and regulatory failures justifying regulation
  + What is “Market Failure”?
    - When an economy has an equilibrium that is not Pareto efficient
    - First Theorem of Welfare Economics: equilibrium of competitive economy is Pareto efficient
  + Graphs (Lecture 3)
  + Natural Monopoly
    - Market failure resulting from:
      * Large fixed costs
      * Declining incremental costs with output
      * Demand variability (idle capacity)
    - Causes lower productive and allocative efficiency
    - Difference in social surplus from competition is deadweight loss from monopoly
  + Network Effects (demand-side phenomenon)
    - Value increases with the number of other consumers
    - Occurs not only with communications services, but platforms
    - Addressed through interoperability mandates and interconnection requirements (between providers)
  + Public Good
    - Product or service for which demand is non-rivalrous
    - Marginal costs of next consumers is zero, but still need to recovers costs (potential to underproduce)
    - Concern to television broadcasting
    - Ex. Watching TV doesn’t impact others ability to watch TV
  + Common Carrier Regulations and Obligations
    - Common Carrier Regulation
      * Reserved for essential services that are public necessity/utility
      * Subject to pervasive regulation to protect public interest since competition not permitted (wasteful)
        + Companies operate in define service territories with licenses
      * Must offer “just and reasonable” rates that mimic competitive market
      * Earn revenues sufficient to cover costs and reasonable rate of return, not monopoly returns
    - Common Carrier Obligations
      * Rates must be non-discriminatory (cost-based differentiation is OK)
      * Overall rate regulation through tariffs (no excessive profits)
      * Control over market entry and exit
    - Obliged to offer reasonable service rates (no excessive monopoly profits)
  + Universal Service
    - Must serve all
    - Funded by explicit and implicit subsidies to achieve “affordability”
    - Essential services
      * Telephone in 1910
    - Broadband in 2010 (in areas of only one provider)

*Federal Communications Commission (FCC)*

* History of the FCC
  + Created by Communications Act of 1934
    - “for the purpose of regulating interstate and foreign commerce in communication by wire and radio…”
  + Combined responsibilities previously residing in the Federal Radio Commission (Title III), plus the Department of Commerce, and the Interstate Commerce Commission (Title II)
  + Original responsibilities
    - Allocate, allot, assign and otherwise manage all non-federal government use of the radio spectrum
    - Regulate interstate communications, common carrier communications and facilities (wired and wireless)
* Organization of the FCC
  + 5 Commissioners, restrictions on political affiliation
  + 5-year term of office, appointed by President, confirmed by the Senate
  + Operating funds from Congress
  + Functions
    - “Ex ante” or command and control regulation
    - Rulemakings to implement legislative mandate
    - Enforce rules/regulations through adjudications
    - Issue licenses
    - Standard setting
* Constraints on FCC Authority
  + Must meet “public interest, convenience, and necessity”
  + Legislative mandates either direction (passing legislation) or indirectly (oversight hearings, reducing budget)
  + Administrative Procedures Act: establishes right to sue the FCC
  + Appeals: petition the FCC for reconsideration or in federal court
* FCC Public Trust Safeguards
  + Outside influence: limits on gifts from outside sources and bribery prohibition
  + Financial restrictions: financial interest in regulated entities and position of close relatives
  + Employment restrictions: matters relating to prior employment and limitations in new employment

*Structure of 1934 Communications Act*

* Title II: Governs common carrier provisions of telephony
* Title III: Establishes regulatory regime for radio spectrum and broadcast services
* Title VI: Addresses cable television and other services over cable

*Federal Communications Commission (FCC) Organization*

* Media Bureau: Broadcast licenses for TV and Radio
* International Bureau: Satellite Systems
* Wireless Telecom Bureau: Cellular Providers
* Office of Engineering and Technology: Unlicensed Spectrum
* Wireline Competition Bureau: Wireline Telephony

*Lessig’s view of generational stages of development for the Internet over time and their implications for civil liberties on the Internet*

*Why has communications been a “regulated industry”?*

* Government limited entry and exit from market using “licenses: or “franchises”
* Government established key economic terms for companies to provide service through “tariffs”
* Government set rates to achieve “universal service”

*Levels of Government Regulation*

* Municipal
* State (Public Utility Commissions – PUCs)
* Federal
  + Executive Branch
    - National Telecommunications and Information Administration (NTIA)
      * President’s principal adviser on telecommunications and information policy issues
      * Controls spectrum used by government
      * Manages grant and loan programs
    - Department of Justice
      * Brings antitrust cases
      * Must approve mergers
  + Legislative Branch (Congress)
    - Broad policy making authority to establish new laws
    - House Energy and Commerce Committee
      * Subcommittee on Commerce, Science and Transportation
    - Senate Committee on Commerce, Science and Transportation
      * Subcommittee on Communications, Technology, and the Internet
  + Judiciary Branch
    - U.S. Court of Appeals (12 Regional Circuits)
      * Most FCC appeals to licensing decisions and rule making proceedings heard by U.S. Court of Appeals for the District of Colombia
    - U.S. Supreme Court
    - Judges: generalists with few resources
  + Fourth Branch: Independent Regulatory Commissions
    - Independent from Executive and Legislative branches through powers delegated by legislative branch
    - Independence within government
      * Commissioners from different political parties
      * Odd number of commissioners, staggered terms, difficult to remove
    - Independent from industry
      * Agency budget from Government, conflict of interest regulations for employees
    - Set policies or rules, through action taken must be under authority of basic laws
      * Must follow general rules as set by Administrative Procedures Act
    - Hear cases, invoke punishments, like judiciary
    - Must give notice, hearing to a violator
      * Actual authority to coerce is not with Agency. If someone refused to follow, then must go to court to enforce.
    - Due process: rates must not be confiscating
      * Courts examine regulations to make sure agency following purpose and will call into question procedural errors
* International (International Telecommunications Union- ITU)

*Independent Regulatory Commissions*

* Federal Communications Commission
* Federal Trade Commission
* Security Exchange Commission
* Federal Energy Regulatory Commission
* Consumer Product Safety Commission
* Nuclear Regulatory Commission
* Commodity Futures Trading Commission

**Unit 2: Achieving Broadband Universal Service through Regulation and National Broadband Plans**

* **Focus of the U.S. National Broadband Plan** 
  + Maximize competition
  + Add broadband to universal service plan
  + Efficient allocation of government assets
* **Universal Service** 
  + Government sponsored subsidy to add or keep users of a desirable service by low rates
  + Principal market/regulatory failures justification
    - Network Effects (demand-side phenomenon)
      * Value increases with the number of other consumers
      * Occurs not only with communications services, but platforms
      * Addressed through interoperability mandates and interconnection requirements (between providers)
      * Lack of market solutions
  + Connect America Fund (CAF) established to fund broadband (fixed and mobile)
  + Universal Service
    - Must serve all
    - Funded by explicit and implicit subsidies to achieve “affordability”
    - Essential services
      * Telephone in 1910
    - Broadband in 2010 (in areas of only one provider)
  + Benefits society by enhancing economic development, democratic participation, and public safety
* **Definition of Broadband for universal service** 
  + Factors
    - Speed (advertised and consistency)/Latency
    - Usage allowances and price
  + Policy benchmark (Section 706)
  + Status of mobile
    - Digital Subscriber Line (DSL) and Fiber-to-the Home
      * DSL is low cost when telephone network is present
      * Low broadbands speeds unless fiber is extended close to customer
      * Speeds are inconsistent
  + Cable Network: Hybrid Fiber-Coax (HFC)
  + Wireless Network: Wireless Internet Service Provider (WISP) or Long Term Evolution (LTE)
* **Local access network technologies** 
  + Types of local access networks
    - Digital Subscriber Line (DSL) and Fiber-to-the Home
      * DSL is low cost when telephone network is present
      * Low broadbands speeds unless fiber is extended close to customer
      * Speeds are inconsistent
    - Cable Network: Hybrid Fiber-Coax (HFC)
    - Wireless Network: Wireless Internet Service Provider (WISP) or Long Term Evolution (LTE)
  + Comparative advantages of different types
    - DSL
      * DSL is low cost when telephone network is present
      * Low broadbands speeds unless fiber is extended close to customer
      * Speeds are inconsistent
    - FTTX- Fiber to the….
    - PON Deloyment
      * One fiber “split” to service around 32 homes
      * Bidirectional – can be sent both ways
    - Fiber Optic Networking Technology
      * Gigabit Passive Optic Network (G-PON)
        + Lowest cost and most broadly deployed FTTP
    - FTTH
      * Hig capacity with unlimited bandwidth
      * Low operation costs (immunity to electrical noise and interference
      * Very high fixed cost
    - Cable
      * Reasonable incremental costs to increase speed
      * High capacity broadband
      * Consistent service speeds
      * Upstream capacity limits
    - Wireless
      * Low cost in last mile
      * Standards lowering equipment costs
      * Speed limitations
* **Comparison of international NBPs** 
  + Difference between broadband/Internet access defined as a legal versus human rights
  + Timeline of focus for NBPs; popularity of NBPs
  + Best practices of NBPs
  + Impact of NBPs on fixed and mobile broadband adoption

**Unit 3: Using Network Neutrality to Insure Access to the Internet**

* Historical Origins of Net Neutrality
  + Carterfone: produced technologies (answering machine, fax, and modem) removing barrier to development of packet switched network, that eventually would become the Internet
  + Computer II established basic vs. enhanced service definition
    - Basic services offered to public is common carrier
    - Enhance services offer content or data processing and is unregulated
  + Service definitions
    - Enhanced services employ computing to
      * “Act on the format, content, code, protocol or similar aspects of the subscriber’s transmitted information, provide the subscriber additional, different, or restructured information, involved subscriber interaction with stored information”
    - Basic Services
      * “pure transmission capability over a communications path that is virtually transparent in terms of its interaction with customer supplied information”
  + Computer II relied on “nonstructural” cross subsidy and nondiscrimination safeguards
  + Telecommunications Act of 1996 renames basic to telecommunications services (Title II), and enhanced to information services (Title I)
* Genesis of Net Neutrality Rules (2005)
  + To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to:
    1. Access the lawful Internet content of their choice
    2. Run applications and use services of their choice, subject to the needs of law enforcement
    3. Connect their choice of legal devices that do not harm the network
    4. Competition among network providers, application and service providers, and content providers
  + FCC’s Preserving the Open Internet Rules in 2010
    1. Transparency: fixed and mobile broadband providers must disclose
       - Network management practices
       - Performance characteristics
       - Terms and conditions of services
    2. No blocking
       - Fixed broadband providers may not block lawful content, apps, or non-harmful devices
       - Mobile may not block lawful websites, apps that compete with their voice/videophone services
    3. No unreasonable discrimination
  + Unreasonable Discrimination
    - Differential treatment of traffic more likely to be reasonable the more transparent it is
    - End-user choice and control central to evaluating reasonableness of discrimination
      * No ban on usage-based pricing
    - Use or application agnostic discrimination probably reasonable
    - “Pay for priority” is a concern
      * Raises barriers to entry
  + Mobile Broadband
    - Rapidly evolving, earlier stage platform
    - Mobile networks present operational constraints not typically faced by fixed broadband
    - Require mobile broadband providers to comply with transparency and no-blocking rules
      * Only prevents blocking of any lawful website or any service that competes with service provided by the mobile operator
      * Other types of blocking (e.g., downloads of large files) may be allowed
    - Unreasonable discrimination rule does not apply
* America needs more broadband, better broadband, and open broadband networks
  + Three overarching policy objectives of 2015 Report and Order
  + Two key findings to justify new rules
    - Broadband providers – both fixed and mobile – have both the incentives and ability to harm the open internet
    - Relatively small incremental burdens imposed by rules outweighed by benefits of preserving the open nature of the Internet
* Retail broadband Internet access service (BIAS) best view as separately identifiable offers of
  + A BIAS that is a telecommunications service (including assorted functions and capabilities used for the management and control of the telecommunication service)
  + Various “add-on” applications, content, and services that generally are information services
* Mobile BIAS is interconnected with public switched network, therefore a Commercial Mobile Service
* BIAS
  + No Blocking – of lawful content, applications, services, or non-harmful devices, subject to reasonable network management
    - Can refuse unlawful content (e.g., child pornography, copyright-infringing materials)
    - Cannot charge edge providers fee to avoid blocking of content, service, or app
    - No minimum level of access standard
  + No Throttling – to impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management
    - Throttling must be reasonably and primarily for network management, no business purposes
    - Prohibits charging edge providers fee to avoid throttling of their content, service, or app
  + No Paid-Prioritization – no management of a broadband provider’s network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management
    - * In exchange for consideration (monetary or otherwise) from a third party
      * To benefit an affiliated entity
    - Priority treatment can cause higher latency, more packet loss, less bandwidth for others
    - If allowed, damage to Internet openness could be difficult to reverse (no “fast lanes”)
    - Allows waiver if significant public interest benefit and no harm to the open Internet
    - No reasonable network management exception – business practice
* Preserving the Virtuous Cycle
  + Internet is level playing field
    - Thrives due to “freedom and openness”
    - No gatekeepers blocking lawful network uses or picking online winders or losers
  + Openness promotes competition
* Modern Title II
  + Forbearance of over 700 rules
  + No unbundling of last mile facilities
  + No tariffing
  + No rate regulation
  + No cost accounting rules
  + Applications of communications act
* New rules address problems of
  + Government control of the internet
  + Decline in investment
  + Loss of employment
  + Weakened online privacy
  + Increasing digital divide
* Policy objectives
  + End utility-style regulation and restore market-based policy approach to preserve internet freedom
  + Require ISPs to be transparent
  + Eliminate Internet conduct rules and other *ex ante* regulations
  + Promote infrastructure investment throughout America
  + Promote innovation and consumer choice among ISP and edge provider services
  + Promote broadband deployment in rural American with goal to eliminate digital divide
* Policy Changes
  + Reinstating classification of BIAS as information service
  + Reinstating classification of mobile BIAS as private mobile service
  + Return broadband privacy authority to the Federal Trade Commission (FTC)
  + Lite-Touch Regulatory Framework
    - Believes *ex ante* regulatory intervention in market is unnecessary verse *ex post* enforcement
    - Eliminating the Internet conduct standard
      * No need for no-blocking, no-throttling, no-prioritization rules
    - Need for transparency rule
* Timeline Summary
  + Computer Inquiry II established 2 Service Types
    - Basic (subject to Title II common carrier regulation of 1934 Act) or Enhanced (ill-define Title I rules) services
  + Telecom Act of 1996 define two entities
    - Telecommunications carriers (Title II) or Information Service providers (Title I unregulated)
  + FCC classified DSL as a telecommunications service (1998)
  + FCC classified cable broadband as an information service (2002)
  + FCC Classified DSL (2005) and wireless (2007) broadband as information services
  + FCC ordered Comcast to new network management approach and transparency based on “ancillary” jurisdiction” (2008)
    - Vacated because FCC failed to identify statutory authority that was reasonable ancillary
  + FCC’s Preserving the Open Internet rules based upon same theory of ancillary jurisdiction (2010)
  + FCC sought comment on reclassification of broadband Internet services in 2010, but adopted Open Internet rules instead
  + Also in 2010, FCC concluded “broadband deployment to all Americans is not reasonable and timely” in Sixth Broadband Deployment Report
  + U.S. Court of Appeals rules in Verizon v. FCC (2014) vacates portions of Open Internet Order (2010) that could only be applied to common carriers
  + FCC’s Protecting and Promoting the Open Internet rules based upon Title II statutory authority (2015)
  + FCC’s Restoring Internet Freedom rules eliminating Title II statutory authority and reclassifying BIAS as information service (2018)
  + U.S. Court of Appeals for District of Columbia affirms most of FCC decision (2019)
* Congestion
  + Effect upon network performance during times when demand exceeds capacity
  + Problem when duration is disruptive to applications
  + Fix by increasing capacity or decreasing demand
  + Types
    - Recurrent congestion
    - Predictable events
    - Unpredictable events
    - Random congestion
    - Bottlenecks usually in low-bandwidth network segments (e.g., access networks) not high (e.g., core ISP networks and networks of ASPs)
  + Indicators
    - Link utilization or load (ratio of demand to capacity)
    - QoS metrics
      * End-to-end packet delay/packet loss/ throughput and jitter
    - QoE – satisfaction of user with performance

**Unit 4: Spectrum Management – Allocation of a Scarce Resource**

* Wireless and Spectrum
  + What are the principles of regulation?
    - Licensing the crowded “public” airwaves
  + How is it assigned?
    - Administrative hearings and auction designs
  + What can I do with it?
    - Goldman Sachs View of the Wireless Future
  + How do we share spectrum?
    - Interference and “unlicensed” bands
* What is Spectrum?
  + Spectrum: conceptual tool to organize a set of physical phenomena
  + Electric and magnetic fields produce (electromagnetic) waves that move through space at different frequencies
  + Set of all possible frequencies called the “electromagnetic spectrum?
  + Subset of frequencies between 3KHz and 300GHz is known as the “radio spectrum” or “radio frequency (RF) spectrum”
* Nature of Spectrum
  + Unique Natural Resource
  + National and International Resource
  + Infinitely Renewable
  + Can be polluted like air or water
  + Scarcity of the Resource – economic value
* Basis of Spectrum Regulation
  + No “ownership” of spectrum”
    - A public resource
  + Need to prevent “harmful” interference
  + Spectrum is a “scarce” resource
* Early Regulations
  + Radio Act of 1912
    - Equipment using spectrum (e.g., for radio stations) must be licensed by the federal government
    - Seagoing vessels must monitor distress frequencies
  + Herbert Hoover creator market-based allocation system (by approving radio system transactions) during the early 1920s as Secretary of Commerce
    - Stopped issuing licenses when market was full
  + In 1926, court overturned Hoover’s extralegal system in *Zenith* decision
    - Extralegal – working outside the law, lacked legal authority
  + Radio Act of 1927 (Legislation)
    - Established Federal Radio Commission
    - Regulate access to spectrum under “public interest, convenience, and necessity” standard
      * Similar to common carriage
    - Public owns spectrum
  + 1927 Act represented political equilibrium among regulators and industry
    - Restricted entry by only utilizing 5% of AM radio market capability
      * Industry interest, allowed them to keep prices from becoming too high, less competition with less users of spectrum
    - “Broadening of the band was disposed of with a finality which leaves little hope for the revival of that pernicious proposition…”
* Rationales for Regulation of Spectrum
  + Managing interference: a negative market externality
  + Rent Seeking
    - “Pirates” and “wave jumpers” after *Zenith* decision in 1926 that eliminated Hoover’s extralegal solution and created the “breakdown” period
    - *Oak Leaves* decision: judge applied homesteading principle to find a common-law remedy to “tragedy of the commons”
      * Established priority-in-use rule (property rights)
* Interference: Negative externality
  + Managing Interference
    - Application of Coase Theorem: if trade in an externality is possible, and there are sufficiently low transaction costs, bargaining will lead to an efficient outcome regardless of the initial allocation of property
      * Competitive environment, no transaction costs (cost it takes to process a transaction or negotiate/bargain a market agreement)
      * Low transaction cost, less friction in the market. Lots of friction is high transaction cost.
    - If FCC specifies property rights, parties should reach an efficient outcome
* Other Rationales for Regulation of Spectrum
  + Consumer Preferences
    - Consumers do not know what’s in their own longer-term interest (i.e., paternalism argument)
    - One person’s consumption of broadcast content may affect another person’s well-being (i.e., externality argument)
      * Negative externalities from violence on TV
      * Positive externalities from children’s TV
* Condensed Timeline
  + Radio Act of 1912 authorized Secretary of Commerce to license users of equipment that communicated via spectrum
  + Radio Act of 1927 established the Federal Radio Commission and that spectrum belongs to the public such that licensees have no property right to continue using it
  + Communications Act of 1934 established the FCC and incorporated the Radio Act of 1927 into Title III
* Spectrum Management
  + Activities associated with regulating the use of the radio spectrum
    - Allocation
    - Service rules
    - Assignment
    - Enforcement
  + Allocation
    - FCC only allocates from private, state, and local government uses
    - National Telecommunications and Information Agency (NTIA) allocates for federal government and military
      * State department coordinates with International Telecommunications Union (ITU)
    - FCC decides license allotment
      * Amount of spectrum or bandwidth in license
  + Status Categories of Allocation
    - Primary Allocations
      * Grant specific services priority in using the allocated spectrum
    - Co-Primary Allocations
      * Occur when there are multiple primary services within a frequency band
      * All have equal rights
      * Station is protected from any others that start operation at a later date
        + Oldest station is protected from other users
    - Secondary Allocation
      * Cannot cause harmful interference to stations of primary services in the band
      * Cannot claim protection from harmful interference from stations of primary service
      * Can claim protection from harmful interference from stations of the same or other secondary service(s) to which frequencies may be assigned at a later date
    - Issues
      * Primary allocation uses poor receivers
        + Get better at discriminating how they select service
        + Ideally only uses allocated band but older receivers tend to us mostly theirs and fall off of others (bell curve)
        + Can cause other users’ interference that greatly affects their service
        + Lack of flexibility, fairly specific for one use
* Service Rules
  + Duration of the license
    - How they can use it
  + Limits on transferability
    - Can’t sell certain licenses they need to be reauctioned by the FCC
  + Maximum power levels
  + Technical standard requirements
  + Build out obligations
* Spectrum Assignment
  + Comparative hearings (up to 1980s)
    - Meet public interest by selecting “most qualified” users
    - Slow, difficult process with high costs, delays, an arbitrary outcomes
  + Lotteries to Qualified Users (late 1980s)
    - Delays in processing large number of applications and fairness concerns as most licenses were quickly “flipped”
  + Auctions (early 1990s – present)
* Spectrum Management Models
  + Command and Control
  + Exclusive Use
  + Commons
* Key Elements of Spectrum Policy
  + Maximizing flexibility of spectrum use to find highest valued use, subject only to interference limitations and reasonable opportunities for access by other users
    - Choice of use, technology, and right to transfer, lease, or subdivide spectrum rights
  + Clear and exhaustive definition of spectrum rights and responsibilities
    - Designated frequency range and bandwidth
    - Geographic scope of right to operate
    - Maximum power output, both in-band and out-of-band
    - Interference protection (maximum level of noise/interferences from other sources)
      * Note uncertainity defining “harmful interference”
* Traditional “Command and Control” Regulation
  + After the communications Act of 1934, FCC decided who and what was worth of using spectrum
  + Granted renewable licenses for specific government-defined uses
  + Service rules define eligibility and service restrictions, power limits, and build-out requirements
  + Users had no ownership right in spectrum
  + Rules designed to prevent “harmful interference”
* Criticisms of “Command and Control” Approach
  + Rigid allocation, allotment, and assignment of spectrum
    - “Static” spectrum management results in spectrum going unused in the frequency, time and/or space dimensions
    - Under-utilizations exacerbated by the use of “worst-case” interference models
    - Can “lock-in” existing uses at the expense of new, more socially-valuable uses
* “Exclusive Use” of Licensed Spectrum Regulation
  + Licensee has exclusive and transferable rights to use of specified spectrum in defined geographic area
  + Flexible use rights with technical rules to protect other users against interference
  + Exclusive rights resemble property rights
    - Coase’s Theorem: with well-define property rights, free market will allocate resources to their most efficient use
    - Owners, acting as “band managers,” can sell or lease spectrum
  + Steps to date: auctions, license flexibility
* “Commons” Model (Unlicensed)
  + Allows unlimited numbers of unlicensed users to share frequencies
  + Usage rights governed by technical standards that set power limits
  + No right to protection from interference
  + Examples to date: amateur radio, CB radio, Bluetooth, Wi-Fi
* “Commons” Model – “Part 15” Rules
  + FCC allows Part 15 devices to use certain unlicensed or licensed bands at very low power levels without prior authorization
  + No protection from interference of others, cannot interfere with licensed users
  + Devices must be certified by FCC as complying to technical standards
* Examples of “Part 15” Bands
  + 1989: Industrial, scientific, and medical (ISM)
    - 900-928 MHz, 2,400-2,483.5 MHz, and 5,725 – 5,850 MHz
  + 1995: Computer to Computer
    - 57-64 GHz
  + 1997: Unlicensed National Information Infrastructure (U-NII) devices
    - 5.15-5.35 GHz and 5.725-5.825 GHz
  + 2002: Ultrawideband
    - 3.1-10.6 GHz
  + 2003: U-NII devices
    - 5.47-5.725 GHz
* Best Conditions for Applying Models (According to FCC Spectrum Task Force)
  + “Exclusive Use”: when spectrum scarcity is high and transaction costs to moving to more efficient uses are low (e.g., bands below 5GHz)
  + “Command and Control”: Prescribing specific usage is necessary for public interest (e.g., public safety)
  + “Commons”: when spectrum scarcity is low and transaction costs to moving to more efficient uses are high (e.g., bands above 5GHz)
* Building Pressures on the Resource (more users, more uses, greater bandwidth)
  + Traditional Solutions to Spectrum Congestion
    - Reallocation
    - Move higher in frequency
    - Increased sharing
    - Improved technology
      * More spectrally efficient technologies (bits/sec/Hertz)
      * More frequency reuse
      * Compression
* Developing the “Commons” by Exploiting “White Space”
  + “White Space”: unused portions of spectrum in terms of frequency, time and space
  + Underlay technologies transmit at power levels below the electromagnetic noise floor (e.g., Ultrawideband)
  + Overlay technologies detect and utilize unused spectrum
    - Dynamic frequency selection capability based on technologies such as GPS for location, beacons, and “listen-before-talk” protocols
* New Sharing Model: Citizens Broadband Radio Service (3550-3700 MHz)
  + Tiered access and authorization framework to share federal/commercial use of 3.5 GHz band
  + Spectrum Access System (SAS) manages access and operations (i.e., automated frequency coordinator based on actual transmissions in band)
    - Uses Environmental Sensing Capability (ESC) sensor network to detect transmissions from Department of Defense radar systems
    - SASs coordinate operations between and among users in three tiers
      * Incumbent Access (Authorized federal users, Fixed Satellite Service (space-to-Earth) earth stations in 3600-3650 MHz band)
      * Priority Access (auction 10 MHz country Priority Access Licenses)
      * A close up of text on a white background

        Description automatically generatedGeneral Authorized Access (Unlicensed)

A screenshot of a cell phone

Description automatically generatedA picture containing clock

Description automatically generated

* Interference Policy
  + Historically: poorly defined standard of “harmful interference”
    - Too stringent or lax guidelines: high opportunity costs
  + Normative goal: Devise guidelines that maximize spectrum value by allowing diverse technologies to flourish and permit “right” level interference
    - Force incumbents to internalize opportunity costs
  + Coase: “the gain from [allowing additional] interference more than offsets the harm it produces”
  + Regulators must balance competing priorities
    - Lightsquared-GPS: need for greater spectrum efficiency vs. need to keep critical infrastructure operable
  + FCC yet to establish comprehensive interference policy
* Goal of Spectrum Auctions: Competition in Wireless
  + Multiple, facilities based networks supporting improved redundancy and reliability
  + Rivalry on coverage, pricing, and service
  + Encourages innovative services, terms, and applications
  + Assign available spectrum to “highest valued” use
    - Maximize consumer value of wireless service less the cost of production
* Using Auctions to Assign Spectrum
  + Encouraging new entry for competition
    - Incumbent advantages of economies of scale and scope
    - Incumbent value driven in part by deterring new entry
  + Should raising revenues be a goal?
    - Can reduce the amount of spectrum
    - Sell to a monopolist
  + Low revenues bad if due to auction design, tacit collusion, or entry deterrence by incumbents
* Market Failures to Consider
  + Less natural monopoly (market concentration) in wireless – but network effects might be sufficient source of concern to merit some regulation
  + Bidders private values may differ from social values (e.g., incumbent includes private value plus value of keeping it away from competitor)
  + Policy instruments impact competition both in the auction and downstream market for wireless services
* Current Setting
  + Spectrum Auctions used to assign and price spectrum since 1994 in U.S.
    - About 90 auctions, raising of $130 billion
    - Goal of economic efficiency: put the spectrum to highest-valued use
  + Policy instruments for competition available to regulators using auctions
    - Set-asides
    - Bidding credits
    - Spectrum caps
    - Band plan design
    - Auction format
    - Antitrust enforcement
* Designated Entities and Bidding Credits
  + FCC auction authority stems from Omnibus Budget and Reconciliation Act of 1993: Revenue maximization is not to be the goal of auctions
    - Section 309(j): FCC should ensure opportunity of small businesses owned by women and minorities, and rural telephone companies (“Designated Entities”)
      * Supreme Court Adarand decision trimmed list to small businesses
  + How do you define “small businesses”? – Large company entering new market?
  + Bidding credits used assuming additional participation can increase revenues
    - Allows government to put a “face value” on some policy goal (e.g., new entrant)
    - FCC auction evidence shows bidding credits typically “bid away” as qualified entities compete for licenses
* Important to Enforce Rules
  + In 2014, Northstar Wireless and SNR Wireless LicenseCo borrowed from Dish in exchange for Dish’s de facto control
    - Also expected to qualify for FCC’s bidding credits for small business (revenue below $40 million)
    - FCC accepted their $13.3 billion in bids but denied requests for $3.3 billion in credits
  + “2G Scam” in India in 2008 when Minister of Communications and IT forced “first come, first served” licensing scheme
    - Illegally undercharged major companies ($28 billion) by tipping off favored companies to conditions required (all happened in matter of hours)
    - In 2011, Time listed scam at #2 of “Top 10 Abuses of Power” list, right behind Watergate
* Sources of Spectrum: Reclaiming Government-Held Bands
  + Government agencies do not internalize opportunity costs
  + President’s Council of Advisors in Science and Technology (PCAST) in July 2012
    - Comprehensive reallocation of federal spectrum not going to happen
    - “Norm for spectrum use… should be sharing, not exclusivity:
  + Industry response: “Gold standard… remains cleared spectrum”
* Why is access to spectrum a challenge for community networks?
  + Spectrum scarcity
  + Inefficient use of spectrum
  + Expense of spectrum access
    - “governments should focus on putting spectrum to its highest and best use, and to consider setting aside spectrum for community and/or local access networks at a reduced cost. Doing so ensures long-term benefits for end users and serves the public interest.”
* Innovative Licensing Approaches
  + Social purpose licensing(set-asides for non-traditional operators
  + Experimental licensing
  + Spectrum auction credits
  + License exemptions and unlicensed use
  + Secondary use and dynamic spectrum sharing
  + Secondary market transactions
* Unit 4 Wrap Up
  + The need for regulation of spectrum and how it has been regulated in the past
    - Spectrum is a scarce resource, owned by the public
    - Need to prevent harmful interference
    - Regulate access to spectrum under “public interest, convenience, necessity” standard
  + How modern spectrum management practices are applied to support mobile wireless applications and how technologies have required these practices to change over time
    - Categories: Allocation, Service Rules, Assignment, Enforcement
    - Spectrum usage models: Exclusive use (licensed), Commons (unlicensed), and Command & Control
      * Circumstances (spectrum scarcity, transaction costs, public interest) favoring each model
    - Technologies permitting more spectrum sharing via time, space, and location (white spaces)
  + The Economics of spectrum scarcity, and how this impacts the market for mobile services and how they are regulated
    - Economics applied to spectrum auctions (promote competition, policy instruments)
    - Coase’s law applied to interference
    - Internalizing Opportunity Costs

**Unit 5: Privacy on the Internet**

* Defining Privacy
  + Privacy: ability (or maybe the ‘right’) of an individual to control their exposure to the rest of the world, and to be able to hide information about themselves
  + Impact of new Information Technologies such as digital storage, processing, retrieval, and distribution
    - Enormous cost reductions and massive adoption
    - Combine, re-use, re-purpose data (data mining)
    - Ability to process data using artificial intelligence (analytics)
  + Raises concerns over use of Personally Identifiable Information (PII)
  + Society’s needs sometimes trump individual privacy
* Privacy and Law
  + No constitutional right to privacy
    - The word “privacy” is not in the Federal Constitution
    - Congress has passed numerous laws
      * Effectiveness under constant debate
      * Problems due to growth of ad-based business models on Internet, trends in data analytics and artificial intelligence
    - Privacy is a function of culture, means different things in different countries
      * Major differences hold implications for global Internet
* Collecting Personal Information
  + Often voluntary
    - Filling out a registration form
    - Registering for a prize
    - Supermarket “Rewards” programs
  + Legal, involuntary sources
    - Demographics
    - Change of address
    - Various directories
    - Government records
* Complications
  + Lots of information floating about online
    - How should we handle concerns over use of this information
    - Who should have access to PII? Who should know?
  + Consumers can benefit from sharing information
  + Consumers may be harmed from sharing information
  + How much should be shared and who should decide?
    - Some laws exist that try to draw this line
* U.S. Privacy Laws
  + 1970: Fair Credit Reporting Act
    - Limits the distribution of credit reports to those who need to know
  + 1974: Privacy Act
    - Establishes right to be informed of personal information on government databases
  + 1978: Right to Financial Privacy Act
    - Prohibits federal government from examining personal financial accounts without due cause
  + 1986: Electronic Communications Privacy Act
    - Prohibits federal government from monitoring personal e-mail without a subpoena
  + 1988: Video Privacy Protection Act
    - Prohibits disclosing a video rental records without customer consent or a court order
  + 1994: Communications Assistance for Law
    - Enhance lawful interception by requiring built-in capabilities in telecom equipment for targeted surveillance
  + 2001: Patriot Act
    - Streamlines federal surveillance guidelines to simplify tracking possible terrorists
* Children’s Online Privacy Protection Act (COPPA) of 1998
  + Enforcement and regulations by Federal Trade Commission
  + What responsibilities operator has to protect children’s privacy and safety online
    - Post clear and comprehensive privacy policy of information practices for PII
    - Provide direct notice to parents and obtain verifiable parental consent before collection
    - Give parents choice of consenting to collection and internal use of PII, but prohibiting disclosing data to third parties
    - Provide parents access to their child’s PII to review and/or have data deleted
    - Give parents opportunity to prevent further use or online collection of child’s PII
    - Maintain confidentiality and security of PII, including taking reasonable steps to release PII only to parties capable of maintaining its confidentiality and security
    - Retain PII for only as long as necessary to fulfill purpose for which it was collected, delete using reasonable measures to protect against unauthorized access or use
  + FTC revised rules in 2012 to require parent consent of ruse of :
    - Geolocation data, photos or videos containing a child’s image, audio files with a child’s voice, screen or online user name
    - Persistent identifier that collects information about a child’s activities on its website or online service
* FTC Proposal: Do Not Track
  + Universal, persistent opt-out across all web sites
  + Easy for consumers to find, understand and use
  + Enforceable: reduces technical loopholes, compliance can be measures
* User-Centric Privacy
  + More complex “subscription” mechanism (risks alienation)
  + Ideal would be software-negotiation, based on user-preferences and machine-readable statement of privacy policies
  + Does assume that the consumer can make an informed decision
  + P3P (Platform for Privacy Preferences Project tin W3C)
    - Language for defining privacy policies (and for expressing private information and privacy statements)
    - Failed effort to date
  + Inrupt/Solid (decentralized web where consumers own their data)
* FTC: Protecting Consumer Privacy in an Era of Rapid Change
  + Objectives and Focus
    - Section 5 of FTC Act prohibits deceptive practices affecting commerce resulting in focus upon:
      * Transparency
      * Honoring consumers’ expectations about the use of their PII
      * Choices by consumers about sharing PUU
      * Obligation of companies that collect PII to adopt reasonable data security practices
    - Privacy Framework
      * Privacy by design – build in privacy at every stage of product development
      * Simplified choice for consumers – give consumers ability to make decisions about their data a relevant time and context, including by Do Not Track mechanisms
      * Greater transparency – Make information collection and use practices transparent
* Fair Information Practice Principles (FIPPS)
  + Created in 1974 as part of the Privacy Act, although not in themselves law, form backbone of privacy law in the United States
    - **Transparency**: there shall be no personal-record systems whose existence is secret
    - **Choice**: individuals have rights of access, inspection, review, and amendment to systems containing information about them
    - **Information Protection**: There must be a way for individuals to prevent information about themselves gathered for one purpose from being use for another purpose without their consent
    - **Data Protection**: Organizations and managers of systems are responsible for the reliability and security of their systems and for the damage done by them
    - **Accountability**: Governments have the right to intervene in the information relationships among private parties
* FTC Privacy Framework
  + Scope: All commercial entities that collect or use consumers data reasonably linked to a specific consumer or device
  + Privacy by Design: Companies should promote consumer privacy at every stage of the development of their products and services
  + Substantive Principles: Companies incorporate privacy protections into their practices, such as data security, reasonable collection limits, sound retention & disposal practices, and data accuracy
  + Simplified Consumer Choice: Companies should simplify consumer choice
  + Practices that Do Not Require Choice: Those practices consistent with context of transaction or company’s relationship with consumer or specifically authorized by law
  + Companies Should Provide Consumer Choice for Other Practices: Offer choice at a time and context in which consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.
  + Transparency: Companies should increase the transparency of their data practices
  + Privacy Notices: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.
  + Access: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use
  + Consumer Education: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices
* European Union’s General Data Protection Requirements (GDPR)
* Definitions
  + Personal Data: information related to a ‘Data Subject’ used to identify person
  + Data controller: entity that determines purposes, conditions and means of processing personal data
  + Data processor: entity that processes data on behalf of Data controller
    - Processing: any operation performed on personal data whether or not by automated means, including collection, use, recording, etc.
* Tracking Technologies
  + Visiting 3 links per site, found Google tracking infrastructure on 92 of top 100 most popular websites, and on 923 of top 1,000 websites
    - Google’s ability to track on popular websites approaches level of surveillance only an ISP can achieve
  + “hundreds of third-party hosts also track users, and under the current self-regulatory regime, it is up to users to investigate these companies’ privacy policies and decide whether to use the websites”
* Industry White Paper Setting
  + Cookie: fundamental infrastructure component of the Internet, but there are concerns that the ‘cookie may be crumbling’
    - Cause excessive Internet traffic
    - “Internet bloat” (web beacons and pixels that deploy cookies slow download times)
    - Regulatory threats
    - Anxiety among consumers and publishers
* State management
  + Method and ability for systems to remember information
  + Cookies used to personalize services and remember preferences for future services
  + Consumer attitudes favor personalized content, advertising, and services
* Guiding Principles for Consumers
  + Single privacy dashboard or place to view state information
  + Universal privacy view or single place to opt in or out
  + Comprehensive privacy controls across all parties
  + Persistent, universal preferences across all devices
  + Detection of non-compliant actors
  + Free online service
* NIST Privacy Framework Webinar
  + Collaborative Development

|  |  |
| --- | --- |
| Attributes |  |
| Outline | 2. Public Comment Periods |
| Discussion Draft | 3. Public workshops |
| Preliminary Draft | 5. Webinars |
| Version 1.0 | |

* + Value Proposition
    - Privacy Framework supports:
      * Building customer trust
      * Fulfilling current compliance obligations
      * Facilitating communication
  + Relationship between Cybersecurity and Privacy Risk
    - **Data**: A representation of information, including digital and non-digital formats
    - **Privacy Event**: The potential occurrence of problematic data action
    - **Data Processing:** The collective set of data actions (i.e., complete data life cycle including collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)
    - **Privacy Risk**: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur
    - **Cybersecurity Risks**: Associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
  + Privacy Risk and Organizational Risk
    - Problem: arises from data processing
    - Individual: experiences direct impact (e.g., embarrassment, discrimination, economic loss)
    - Organization: resulting impact (e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)
  + Role of Privacy Risk Assessment
    - Cross-organizational set of processes that help organizations understand how their systems and services may create problems for individuals, and how to develop effective solutions to manage such risks
  + Privacy Risk Assessments
    - Information to weight benefits of data processing against risks and determine appropriate response (proportionality)
    - Outcomes
      * Mitigating the risk (e.g., technical and/or policy measures that minimize the risk to acceptable degree)
      * Transferring or sharing the risk (E.g., contracts can share or transfer risk to other organizations, privacy notices/consent mechanisms means of sharing risk with individuals)
      * Avoiding the risk (e.g., organizations may determine risks outweigh benefits, forgo data processing)
      * Accepting the risk (e.g., organizations may determine problems are minimal/unlikely, therefore benefits outweigh risks)
  + Appendix D: Key Privacy Risk Management Practices
    - Organizing preparatory resources
    - Determining privacy capabilities
    - Defining privacy requirements
    - Conducting privacy risk assessments
    - Creating privacy requirements traceability
    - Monitoring changing privacy risks
  + Privacy Framework Structure
    - The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk
    - **Profiles** are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk
    - **Implementation Tiers** help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile
  + Privacy Framework Core
    - **Identify-P:** Develop the organizational understanding to manage privacy risk for individuals
    - **Govern-P:** Organizational governance to enable ongoing understanding of organization’s risk management priorities
    - **Control-P:** Enable organizations or individuals to manage data with sufficient granularity to manage privacy risks
    - **Communicate-P:** Enable reliable understanding and engage in a dialogue about how data are processed and associated privacy risks
    - **Protect-P:** Develop and implement appropriate data processing safeguards
* Establishing the Baseline: Size of U.S. Digital Economy
  + Digital economy: all digital goods and services
  + Accounted for 6.9% (1.35 trillion) of gross domestic in 2017 according to statistics released by Bureau of Economic Analysis (BEA)
  + Supports 5.1 million jobs in 2017 (3.3% of total U.S. employment of 152.1 million jobs)
  + Employees earned $132,223 in average annual compensation in 2017, compared to $68,506 per worker for the total company
* Search Costs
  + Privacy rights: right not to be annoyed
  + “excess search costs” arise because seller has too little information about the buyer
  + If seller knows precise buyer interest in product, make better decision about providing product information
* Secondary Users of Information
  + Information of a transaction from original seller and third party may not have well-aligned incentives
    - “Externality” present: actions of third party may impose costs on original buyer, which the seller ignores
    - Mitigation: allow buyer to forbid all secondary transactions in his personal information
  + “Annoyance” improved with clear communications between buyers and sellers
* Incentives Involving Payment
  + Sometimes buyer’s revealing information is detrimental (e.g., smoker buying life insurance)
  + People who have negative characteristic lack incentives to reveal, but people who don’t have good incentives to reveal
  + Solution: Seller constructs transaction in way that reveals information (e.g., discount for non-smokers)
* Contracts and Markets for Information
  + Problems arise due to lack of information
  + Use of property rights could be used to cause more efficient transactions
  + Allow contracts that assigns property rights to one’s PII, defining how individual chooses to sell, or more property, rent, that info
    - For limited times and specified purposes
    - Information could not be resold, or provided to third parties, without that individual’s explicit agreement
    - Could even develop market for PII
      * Today, property rights held by those who collect and compile PII – not by individuals themselves (e.g., recall results of Web Census trackers)
      * FIPPS would automatically implement property rights in individual information
* FIPPS for Certified Information Privacy Professional (CIPP) Certification
  + Privacy Notice must include:
    - Legitimate name and physical address of entity collecting data
    - Type of data collected
    - How collected data will be used
    - Any potential third-party disclosure or secondary use of PII
  + Individuals must be able to consent or reject certain uses of PII, particularly for secondary uses and marketing purposes
    - Two main mechanisms: Opt-in (action required to START) and Opt-out (action require to STOP)
    - Individual must be able to view their consent options and change them at any time
  + Individual must be able to view data an entity has on record
    - Must be able to correct incomplete or false information contained in their file
    - Access to data must be granted within a reasonable time frame and a minimal cost
  + Data must be accurate, up-to-date, not stored longer than needed
  + Security of data must be maintained using physical, technical and administrative safeguards to protect against unauthorized access, use, disclosure and destruction
  + Safeguards should be implemented in proportion to security risk, with greater risks using greater resources and stronger protections
  + Individual must be able to file complaints with the entity to have their issues addressed
    - Should be mechanism in place to ensure compliance with privacy standards, either through self or government
* Assignment of Rights
  + Economic Solution
  + Determine baseline assignment of rights, allow individuals to trade rights if they desire
    - If not transactions costs in trading or negotiation, initial assignment of privacy rights is arbitrary from the viewpoint of economic efficiency

**Unit 6: Cybersecurity**

* Cyberspace: Artifacts based on, or dependent on, computer and communications technology, information these artifacts use, store, handle, or process, and how these various elements are connected
* Cybersecurity (security in cyberspace): technologies, processes, and policies that help to prevent or reduce negative impact of events in cyberspace
  + Result of deliberate actions against information technology by hostile or malevolent actor
* Factors creating cybersecurity issues
  + Presence of malevolent actors in cyberspace
  + Societal reliance on IT for many important functions
  + Inevitable presence of vulnerabilities in IT systems that malevolent actors can exploit
  + Cybersecurity is a never-ending battle, and a permanently decisive solution to the problem will not be found in the foreseeable future
* Security Concerns
  + Fast growing “Attack Surface” to valuable information
    - Smartphones
    - Cloud data
    - 50-60B Internet of Things devices by 2020
* Problems cannot be solved only with technical solutions
  + Improvements can considerably reduce damage due to cybersecurity breaches
    - Efforts to more widely use what is known about improving cybersecurity
    - Efforts to develop new knowledge about cybersecurity
  + Publicly available info and policy actions insufficient to motivate adequate sense of urgency
  + Tradeoffs to improve cybersecurity inevitable, have to be accepted through political and policy-making processes
* Key Tradeoffs
  + Economics
  + Innovation
  + Civil Liberties
  + International relations and national security
* Why should society care about cybersecurity?
  + What are effective approaches to state-of-the-art cybersecurity challenges?
  + What are the essential cyber vulnerabilities and threats upon which Society requires awareness?
    - Requirements for cyber hygiene?
    - Requirements for cybersecurity use education?
  + Why such little progress despite significant policy responses?
* Public Policy Concerns
  + Cybercrime
  + Loss of privacy
  + Activism
  + Misappropriation of intellectual property
  + Espionage
  + Denials of service
  + Destruction of cyberphysical systems, critical infrastructure, public confidence
  + Threats to national security and cyber war
* Computing Technologies
  + A fundamental concern:
    - “Although it may be possible to show that the program does what it is supposed to do… it is impossible to show that it will never do what it is not supposed to do with all possible inputs”
    - Eddie Tipton sentenced to 25 years in 2017 for rigging lottery system to win more than $2M. He designed code that predicted winning numbers in some games on three days of the year.
* Digital Representation of Information
  + Information is inherently anonymous
    - Activist/Hacktivist/white hat/black hat
    - Authentication associations can always be separated from data in principle
  + How to distinguish sequence of bits between program and data?
  + Enables cryptographic methods
* Encrypted Traffic Paradox
  + Rise of encrypted traffic decreases effectiveness of security analytics
* Data exfiltration: unauthorized transfer of data from a computer
* Cyber Exploitation: Action to exfiltrate digitally stored information to unauthorized parties
* Cyberattack: action intended to cause denial of service or damage/destruction of stored/transiting info
  + DDOS, botnets
* Cyber Penetration
  + Access
    - Remote access/close access (e.g., part of supply chain)/social access
  + Vulnerability
    - Accidental flaws/intentional flaws/configuration errors
    - “Zero day” vulnerability
* Characterizing Threats
  + Advanced Persistent Threats (APTs)
    - Focused target/customized to specific security configuration/difficult detection
  + Malevolent actors
    - Keep trying/use deception/persuasion good option/will not go away
* What about antivirus software?
  + Protects against known attacks
  + Cybercriminals can now quickly change attack signatures (e.g., using polymorphism malware with small changes)
  + Antivirus and firewalls not enough to prevent users from installing malware on their devices
* Future Trends
  + Combination of perimeter-based, endpoint and network based security
    - Cloud-based endpoint detection and response (EDR)
    - Perimeter and network security algorithms will run as virtual applications in cloud to find and prevents APTs
* 2020 End-to-End Security
  + Endpoint introspection on qualifying devices
  + Permission-based access using biometrics and flexible encryption levels
  + Security analytics for real-time APT detection and mitigation
  + Security information and event management
  + Software defined networking
  + Collaborative threat intelligence and sharing
* End-to-End Principle Debate Over Security in Core
  + End-to-End Preservationists
    - More testing and validation needed against inadvertent disruptions to QoE (speed)
    - Security services responsibility of individual applications
  + Favor Security in Core
    - Embed security services into protocols and active in packet switching layer (e.g., monitoring and remedy)
    - Applications-based security is burden on end users
* Approaches to Improving Security
  + Reducing reliance on ITL balancing advantages vs. security risks
  + Knowing that security has been penetrated
    - Detection: signature checks (morphing and zero-day concerns), behavioral signatures (false positives)
    - Assessment: scale of attack, targets, damage, foreign involvement, attribution
  + Defending a System or Network
    - Reducing number of vulnerabilities (patching, design)
    - Eliminating/blocking unnecessary access paths
    - Whitelisting software
  + Potential conflicts with performance and functionality (e.g., backward compatibility bundles known vulnerabilities)
* Technical Sidebar: Saltzer and Schroeder Design Principles
  + Economy of mechanism: Keep it simple and small
  + Fail-safe defaults: Access based on permission rather than exclusion
  + Complete mediation: All access checked for authority
  + Open design: design not secret
  + Separation of privilege: where feasible, two keys to unlock
  + Least privilege: user operations with least set of privileges necessary
  + Least common mechanism: minimize common mechanisms for users
  + Psychological acceptability: ease of use human interface
* Ensuring Accountability
  + Individual Authentication and access control
    - Ensuring only authorized parties perform certain actions
    - Facilitating accountability
    - Authentication process relied on something you know (password), have (two-factor), or are (biometrics)
  + Organizational Authentication
    - Certificate authorities: secret decryption/public encryption keys
  + Forensics
    - Examine computer hardware, audits of system logs, statistical/historical analysis of message traffic, interviews with system users
* Building Capacity for Containment, Recovery, and Resilience
  + Containment: limiting effects of cyber attack (sandboxes, heterogeneous computing systems)
  + Recover: repair by system restoration to earlier point in time
  + Resilience: performance degrades gradually rather than catastrophically (redundancy)
* Employing Active Defenses
  + Cyber deception for defensive purposes (honeypots)
  + Disruption: reduce damage by affecting operation of computer systems causing attack (disabling botnet)
  + Preemption: anticipatory self defense
* Economic Approaches to Enhancing Cybersecurity
  + Use existing market mechanisms but with improved flow of info (e.g., better info about threats and vulnerabilities)
  + Insurance (incentives for lower premiums)
  + Liability accountability
  + Direct Regulation (e.g., adoption of best practices)
* Other Policy Concerns
  + Innovation
    - Reducing time to market vs. security by design
    - Ease of use, interoperability, and backward compatibility vs. security
  + Civil liberties
    - Privacy/free expression (concerns for strong packet authentication)/due process
* International Relations and National Security
  + Internet governance = management/coordination of technical elements of Internet (e.g., DNS)
  + Cybersecurity vs. surveillance tradeoffs – managing incompatible objectives
    - Communications Assistance for Law Enforcement Act (CALEA) of 1994 – Telecom industry must design, develop, and deploy systems that support law enforcement requirements for electronic surveillance
      * The Athens Affair
    - Norms of cyberspace behavior
      * Collecting national security/foreign policy info = espionage (permitted)
      * Collecting economic/business interests = theft of intellectual property/trade secrets
  + Arms control in cyberspace unlikely to be feasible (due to verification challenges, legitimate uses to improve defenses, etc.)
    - Banning cyber exploitation goes beyond current international laws
  + Confidence building measures for ICT to provide stability and mutual understanding
  + Managing a global supply chain
  + Role of offensive operations in cyberspace
    - U.S. would respond using all available means (diplomatic, military, economic…)
    - Laws of war apply, though no published military doctrine
    - Requires presidential approval due to significant consequences
* Presidential executive order 13636: Improving critical infrastructure Cybersecurity
  + Develop technology: neutral voluntary cybersecurity framework
  + Promote and incentivize the adoption of cybersecurity practices
  + Increase volume, timeliness and quality of cyber threat information sharing
  + Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  + Explore the use of existing regulation to promote cyber security
* Presidential executive order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  + Policy to solve four problems
    - Secure federal networks
    - Encourage collaboration with industry to protect critical infrastructure
    - Strengthen deterrence posture of the United States and build international coalitions
    - Build a stronger cybersecurity workforce
* Section 1 Cybersecurity of Federal Networks
  + Department/Agency heads accountable for managing cybersecurity risk
    - Undertake risk management measures to commensurate with magnitude of harm
    - Use NIST Cybersecurity framework and provide report in 90 days
  + Focus on assessing and reducing risk to improve cybersecurity using best practices, tools and services that are cloud-based
  + Determine to use shared IT services such as email, cloud and cybersecurity services
    - Gather info on IT architectures and plans to determine technical feasibility and cost effectiveness of transitioning all agencies to one or more consolidated network architectures and shared IT services
* Section 2 Cybersecurity of Critical Infrastructure
  + Focus on how to best support cybersecurity of critical infrastructure through policies and stakeholder engagement
  + Discuss with stakeholders how federal capabilities can best support designated critical infrastructure
  + Commerce and DHS to promote actions to reduce risks from distributed, automated attacks (i.e., botnets)
  + Assess potential scope/duration of power outage associated with significant cyber incident against electric grid
* The Cybersecurity Framework
  + Includes a set of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks
  + Provides a prioritized flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk
  + Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards developing organizations
  + Is consistent with voluntary international standards
* The framework is for organizations
  + Of any size, in any sector in (and outside of) the critical infrastructure
  + That already have a mature cyber risk management or cybersecurity program
  + That don’t yet have cyber risk management or cybersecurity program
  + Needing to keep up-to-date managing risks, facing business or societal threats
  + In the federal government, too… since it is compatible with Federal Information Security Management Act (FISMA) requirements and goals
* Cybercrime Economics
  + “Information is secure when it costs more to get it than it’s worth”
    - Kevin Poulsen (“Dark Dante”, now Wired contributing editor)
  + Cybercrime more lucrative than traditional crime
  + Online markets for tools
* Key Economic Concepts
  + Misaligned incentives
    - Parties making security-efficiency tradeoff are not who incur costs when attacks occur – between those responsible for security and those who benefit from protection
      * Medical records in hospitals
      * Electric utilities control systems
      * Online banking
    - Tradeoff between short-term efficiency and long-term vulnerability of system resilience
    - All can lead to suboptimal choices due to misalignment
  + Information Asymmetries
    - Lack of available data needed to guide security investment
    - Who knows the costs of cyber threats?
      * Banks do not disclose online fraud losses
      * Businesses want to protect their reputation, not draw attention to vulnerabilities
    - Is security software a “ market for lemons”?
    - Decision making under uncertainty
      * Asymmetry means level of investment likely inefficient
  + Market externalities
    - Entities actions have side effects on others
    - Race for network effects often involves insecure software pushed to market; and slow adoption of secure upgrades (DNSSEC/S-BGP)
      * SSH/IPSec provide immediate internal benefits
    - Negative externalities in attacks lead to under-investment to prevent societal risk
      * Cyber security a public good?
    - Free riding likely when security depends on the weakest link in the chain (why invest if others don’?)
* Solution for market Failures
  + *Ex ante* safety regulation
    - Firms adopt best practices and test compliance (Financial Services Modernization Act, Health Insurance Portability and Accountability Act, etc.)
  + *Ex post* liability
    - Section 5 of Federal Trade Commission Act grants FTC authority to take action against *unfair or deceptive* *acts* that affect commerce
  + Information disclosure
    - Establish information sharing and analysis centers (ISACs)
      * Nonprofit organizations gathering info on cyber threats to critical infrastructure and providing two-way sharing of info between private and public sectors
  + Cyber insurance
    - Mechanism to manage risk (insurance companies can offer incentives for precautions/collect data on incidents/smooth costs)
    - Global market projecting strong annual growth of 25% through 2025 (from $4.6B in 2017)
      * Standalone cyber insurance rate approaching 40%
      * Cyber insurance purchases grew most among hospitality and gaming (67%) and education (34%) organizations
      * Average limits purchased grew 11% to $20.9M
      * Among companies with revenues above $1B, average limits increased by 25% to $62.4M
* What Does Cyber Insurance Cover?
  + Also known as Cyber Risk or Cyber Liability Insurance
  + Covers costs associated with an actual data breach where customers’ PII exposed or stolen from firm’s data network
    - Forensic investigation to determine what occurred, how to repair damage, how to prevent similar breach in future
    - Business losses due to network downtime, business interruption, data loss recovery, costs involved managing crisis, and repairing reputation damage
    - Data breach notifications to customers and other affected parties
    - Legal expenses associated with release of PII and IP, legal settlements, regulatory fines (may include costs of cyber extortion)
* Economic Approaches to Enhancing Cybersecurity
  + Use existing market mechanisms but with improved flow of info (e.g., better info about threats and vulnerabilities)
  + Insurance (incentives for lower premiums)
  + Liability accountability
  + Direct regulation (e.g., adoption of best practices)
* Other policy concerns
  + Innovation
    - Reducing time to market vs. security by design
    - Ease of use, interoperability, and backward compatibility vs. security
  + Standards setting and certification
    - Good practices codified in standards, public recognition of conformance can improve competitive position
  + Civil liberties
    - Privacy/free expression/due process