Cybersecurity Paradigm Shift

Catherine J.K. Sandoval

Associate Professor

Santa Clara University School of Law

Digital Civil Society Lab Speaker Series,

Stanford University,

February 4, 2020

The Internet Origin Story: Connecting the Galactic Network

J.C.R. Licklider of MIT in August 1962 writes memos conceiving a "Galactic Network" of interconnected computers that allows quick access to data and programs from any site

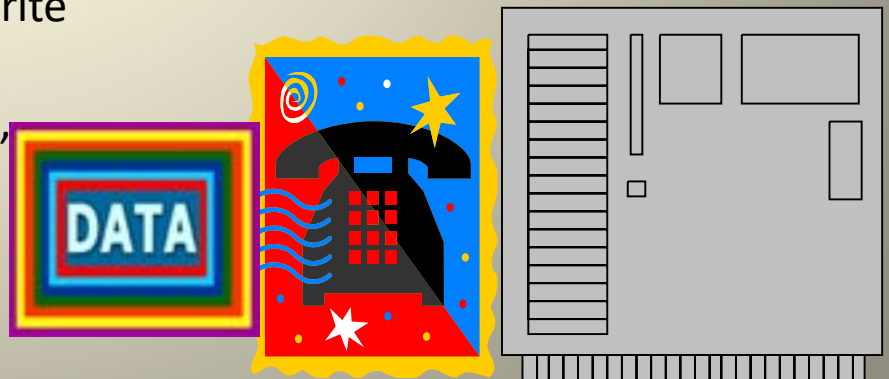
Licklider works at DARPA as the first head of the computer research program, October 1962.

?

How would computers communicate?

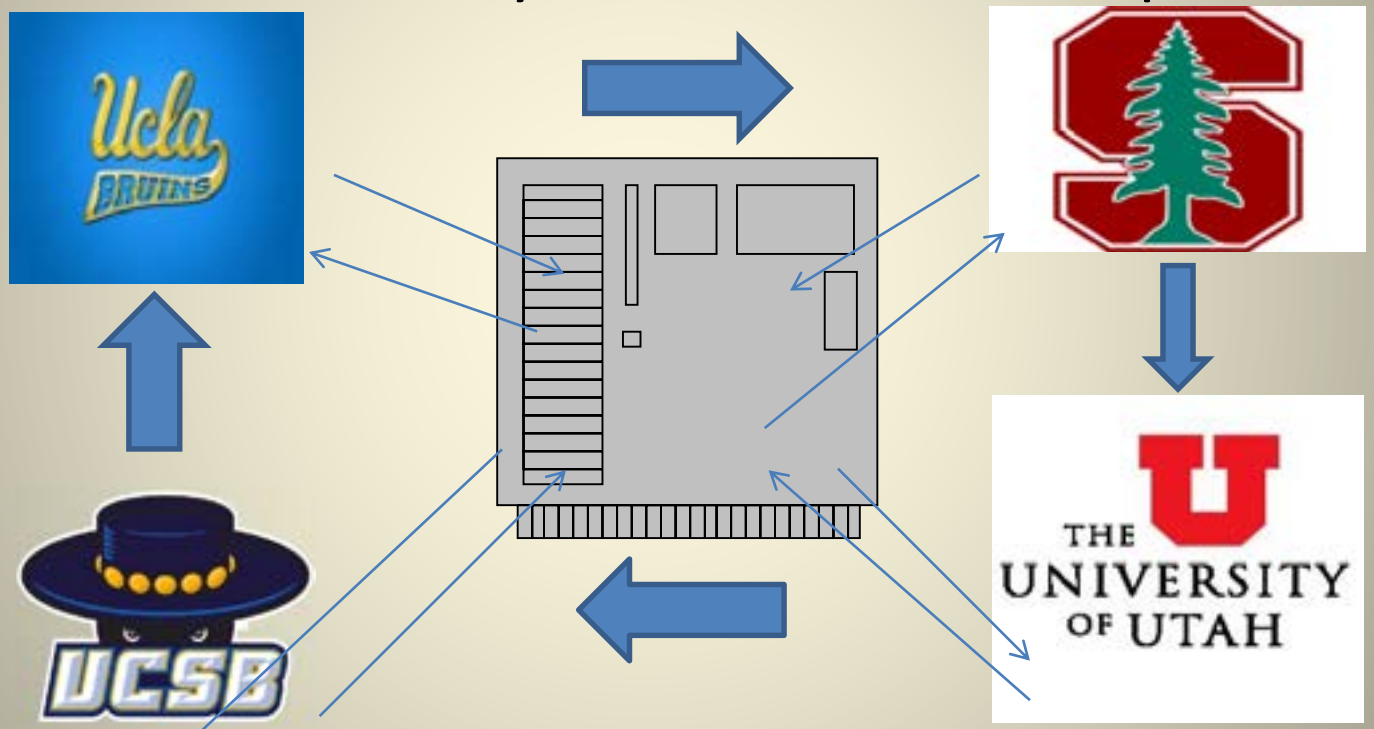
Leonard Kleinrock at MIT, NPL, Rand, and others write papers and books on Packet Switching, Communications using packets rather than circuits, 1961-1967

BEST EFFORTS STANDARD for DATA Exchange!



Internet Evolution: From Cold Warrior to Engine for Innovation, 1969

ARPANET Connects Computers at UCLA, Stanford, UC Santa Barbara, and the University of Utah, 1969: The public Internet goes live!



Network access initially restricted to American defense circles and the government-funded scientific community.

More universities and research centers link, 1969-1984

The Internet's Journey from Closed to Open, 1985-1991

- **NSFNET, National Science Foundation Network,** funded by the Federal Government to support the Internet's backbone and development, 1985
- ***NSFNET had an Acceptable Use Policy (AUP) that prohibited use of the NSFNET for purposes not in support of research and education***
- Experimental commercial uses allowed in 1988, MCI Mail, Compuserve, Sprint, to enhance research and educational uses
- AUP changed in 1990 to allow NSFNET "to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work."
- NSF funded Network Access Points ("NAPs") for exchange of traffic and required the privatized NSFNet backbone to connect to them
- **High Performance Computing Act of 1991 (HPCA),** 15 U.S.C. 5501 (Dec. 1991) (**Senator Al Gore, author, signed by President George H.W. Bush)**.
- **Commercial networks allowed to connect with NSFNET, 1995**

Internet Models: Open, Closed, or Controlled System

- **The Internet as an Open System: Anyone can connect, download and share:**

- Data sent on best efforts basis

- **The Internet as an Closed System:**
- Only certain parties allowed in (the early Internet).

Cf. Closed System, a Fortress Open only to a few *vs*. Open System

- **It's all about Control**:
- Parties who control technical access to the Internet can also limit openness (Internet Service Providers, ISPs), Internet backbone carriers (Internet traffic carriers).
- Regulatory debate about allowing ISPs to provide priority Internet access to some parties upon payment arrangements with ISPs

Internet Models: Library of Alexandria or Modern Sharing Common Room

- ***Cf.* The Internet and the Great Library of Alexandria, Egypt:**

- The Supreme Court's 2003 case, *American Library Assn. v. US*, 539 U.S. 194, characterized the Internet as "simply another method for making information available in a school or library," "no more than a technological extension of the book stack."

- **The Internet as the driver of innovation by enabling sharing:**

- In 2014 the D.C. Circuit concludes the Internet drives a "virtuous circle" of innovation enabling people to access, share, and distribute, Verizon v. F.C.C. 740 F.3d 623, 628 (D.C. Cir. 2014)

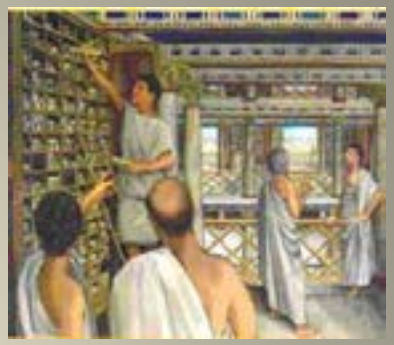
Internet Models Drive Democracy

- First White House Web Site Launched, 1994, President Bill Clinton
- More government agencies, non-profits, and businesses launch web sites

- Google founded, 1998
- Facebook launched 2004
- YouTube founded 2004
- Twitter launched 2006
- **Tahrir Square, Egypt, 2011**

- In the words of one protester, Fawaz Rashed: "We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."

The Internet Evolves in the 21st Century as a Democracy, Civil Society, Educational and Economic Dialogue Platform



- **More government agencies move registration, Voter information, and other functions to the Internet**
- **More companies limit job applications to the Internet**
- **More social media sites**
- **Political candidates, organizations, and individuals use the Internet to organize and distribute their messages, collect, analyze and report data**

- *Packingham v. North Carolina*, 137 S.Ct. 1730 (2017):
- "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the "vast democratic forums of the Internet" in general, and social media in particular."

Democracy Goes Social: # Speak & Organize

- The Internet including social media platforms enable new means to speak and organize
- Social media both drives and reflects the news

- Social media can drive civic organizing efforts including participation in administrative proceedings
- Social media companies such as Twitter and Facebook deleted hundreds of alleged Bot and malicious accounts in 2018.

- FCC 2018 net neutrality repeal Order did not consider impact of paid priority on democracy, civil justice, critical infrastructure, education, health, and many other key values and sectors

Social Media Enables Public Safety

- **The Internet enables one to many and many to many communication daily including during public safety emergencies**

Flickr Photo of Mumbai Attack, 2008

- Survivors of Terrorist Attacks in Mumbai in November 2008 Used Twitter and Flickr to Communicate Incident Details and Report their Safety

- Students in Parkland, Florida use the Internet including social media in February 2018 to inform the public including public safety officials about the shooting ongoing at Marjorie Stoneman Douglas High School

Internet Video Enables Public Safety

- Internet used by the public during fires, *e.g.* the Camp Fire in Paradise, California

The Daily Dot, Family Post Evacuation photo from Camp Fire,
Paradise, California, November, 2018

- FCC Net Neutrality and Internet rulemakings have given little attention to public Internet use including video and social media use for public safety
- Public Safety is more than the ability of the public to contact first responders and first responder communication

The Cat Video Paradigm Frames Internet Law and Regulation

- The “Cat Video Paradigm” frames FCC and legal views of public use of video on the Internet
- *Verizon v. FCC*, description of the Internet depicts a cat video loading.

Internet Cat Video Festival TribLive

Why Cats Rule the Internet, San Jose Mercury News, Feb. 2019

- The FCC only considers cached video in net neutrality repeal
- Video increasingly used to communicate public safety, *e.g.* Videos of the Camp Fire in Paradise, California, sharing evacuation routes and fire status; Videos of police stops and shootings, Videos of Flooding and river status

Sectors of the U.S. economy and society intertwined with the Internet

Jobs, Professions

Transportation

Energy, Water & Critical Infrastructure

Government Access & Services including Public Safety

Other Sectors

Non-profits, Civic & Church Organizations

Manufacturing

Communications & media

Agriculture

Health

Education

Democracy, Public Opinion, Public Organizing, Voting

Commerce

Critical Infrastructure Sectors designated per Critical Infrastructure Protection Act, 2001,

Chemical
Commercial Facilities
Energy
Water & Waste Water
Government Facilities
Defense-Industrial Base
Financial Services
Critical Manufacturing
Dams
Communications & media
Food & Agriculture
Emergency Services
Transportation Systems
Healthcare & Public Health
Information Technology
Materials
Nuclear Reactors

"CIPA defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The Hacker-Paradigm Frames Cybersecurity Analysis

- The U.S. Department of Homeland Security's March 2018 warning regarding hackers probing the energy grid underscores the importance of cybersecurity to energy reliability and national security. Hacker threats to energy are real and persistent.
- The "***Hacker Paradigm***" obscures other systemic threats to energy reliability and cybersecurity
- *Traditional cybersecurity techniques do not work against a user's own ISP: You can't throw a firewall over your ISP!*
- An ISP that slows or degrades signals used for energy system operation, maintenance, planning, and other activities may compromise energy system reliability, safety, and functionality.
- ISP Network Management free of Net Neutrality Rules creates a supply chain vulnerability that requires cybersecurity vigilance

Cybersecurity & Cyberattacks, Defined

- "Cyberattacks" are defined by U.S. National Research Council as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."
- "Cyber exploitation" is defined as intelligence-gathering activity
- Cyberattack may fall under International Laws regarding the "use of force" and "armed attack" under the United Nations Charter
- The law of armed conflict (legality of going to war) (jus ad bellum) and law governing behavior during war (jus in bello) apply to cyberattack
- Gaps in coverage for non-state actors
- **Net neutrality debate focuses on ISP governance**. *Must consider cybersecurity implications of ISP paid priority, blocking, throttling, and governance policies*

Cybersecurity Alerts
Cybersecurity and Infrastructure Security Agency

- CISA warns in e.g. May 2018 that foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide
- CISA warns in March 2018 that the Russian Government is targeting organizations in the energy, nuclear, water, aviation, commercial facility, and critical manufacturing sectors
- https://www.us-cert.gov/ncas/alerts

Cybersecurity and Cyberattack Governance Gaps

Transmission Grid

Internet-Enabled Distributed Energy Resources Make the Grid Smart and Increase Reliability and Safety

Distribution Grid

- **Cybersecurity for Federal Agencies and Data required by 6 US Code 1523**
- **International Cybercriminals Subject to 6 US Code 1531**
- **Emergency Services and Health Care Services Encouraged to Develop Cybersecurity, 6 US Code 1532-1533**
- ***Energy is the Only Sector with Mandatory Federal Cybersecurity Requirements***

Cybersecurity is Critical to Energy Reliability

"***Energy-Internet Nexus***" created by regulatory and private sector investment decisions over the past 25 years, embedding the Internet into the energy system






- The Energy-Internet Nexus enables integration of distributed energy resources (DERs) such as solar photovoltaic (PV) systems, energy storage, and demand response supported by devices connected through the Internet of Things (IoT).
- The Internet creates important tools for electric grid visibility and control
- The Internet is increasingly critical for grid operations, resource entry and dispatch necessary to achieve environmental goals and combat climate change
- The Internet opens opportunities and cybersecurity vulnerabilities.

Internet Service Providers Ask for Permission to Collect Tolls

- **Verizon's lawyer argued to the D.C. Circuit** "but for [the FCC's *2010 Open Internet Order*] rules we would be exploring commercial arrangements" to be paid to prioritize certain Internet traffic.

Internet Service Providers have Gatekeeper Power over the Internet

- Professor Paul Ohm observed an “ISP's opportunity to invade user privacy stems from network architecture. The ISP operates the network chokepoint--its computers stand between the user and the rest of the Internet--and from this privileged vantage point it has access to all of its users' private communications.”*

- When an Internet subscriber connects to its ISP, the subscriber’s data crosses through the ISP’s network to reach other Internet endpoints.

- ISPs have the technical capacity, financial incentives, and with the FCC’s 2018 net neutrality repeal the legal authority under federal law to act as ***Information Intermediaries*** to control access to their gateways to the Internet in the ISP’s Financial interest

*Paul Ohm, THE RISE AND FALL OF INVASIVE ISP SURVEILLANCE, 2009 U. Ill. L. Rev. 1417 (2009)

FCC 2015 Open Internet Decision recognizes threat of ISP gatekeeper role

- The D.C. Circuit in 2014 found that ISPs have "gatekeeper" power to control traffic crossing their network. Verizon v. F.C.C., 740 F.3d 623, 628 (D.C. Cir. 2014).

- The *FCC's 2015 Open Internet Order* found:
- "Broadband providers have both the incentive and the ability to act as gatekeepers standing between edge providers and consumers" and can undermine the "virtuous cycle" of innovation the Internet drives.
- "As gatekeepers . . . [ISPs] can block access altogether; they can target competitors, including competitors to their own video services; and they can extract unfair tolls

Cybersecurity and Public Safety Risks of Net Neutrality Repeal

- **Data slowed by ISPs to accommodate paid priority traffic may be delayed with no safeguards for non-priority data or users**
- **If data is slowed too much program execution or function will fail**
- The FCC imposed no safeguards on ISP traffic to limit slowdowns or prevent traffic failure due to accommodating fast-lane paid priority traffic
- The FCC does not require ISPs to disclose the parties who received priority, the terms or price of priority, and consequences for other users
- Question: ***Are ISP incentives to avoid customer dissatisfaction with traffic delays or slowed traffic enough to prevent behavior harmful to consumers and public welfare?***
- **Question:** ***Is information about paid priority enough to safeguard the Internet and its users? How much information?***

Risks of ISPS as Gatekeepers Information Intermediaries

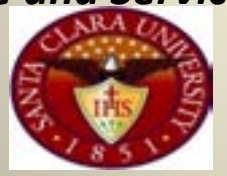
Discuss Risks of an ISP as an Unregulated Information Intermediary to:

Democracy

Public Safety

Critical Infrastructure and Services

Education



Health

Other sectors, Internet of Things

Internet of Everything and Everyone

FCC 2017-2018 Internet Freedom Proceeding Fails to Consider Public Safety in Net Neutrality Repeal

- The FCC's founding statute, the Communications Act of 1934 Require it to consider public safety

- The Wireless Communication and Public Safety Act of 1999 § 3, 47 U.S.C. § 615 requires the FCC to consider public safety in encouraging reliable wireless telecommunications networks and enhanced wireless 9-1-1 service
- Nuvio Corp. v. F.C.C., 473 F.3d 302, 307 (D.C. Cir. 2006) recognizes the FCC's duty to consider public safety in its rulemakings



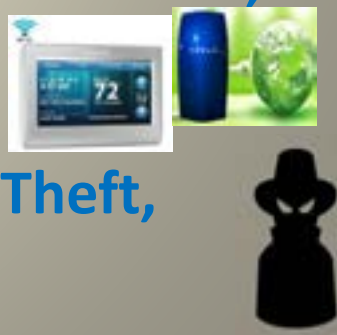
The 2010 and 2015 Open Internet Decisions Cite Public Safety as a Reason to Adopt Net Neutrality Rules

- The FCC's *2015 Open Internet Order,* ¶ 126, n. 291, adopted rules prohibiting paid priority to protect public safety and universal service, citing CPUC Commissioner Catherine Sandoval's comments

- The Order also cited protecting free expression, eliminating artificial barriers to entry, distorting the market, harming competition, harming consumers, and discouraging innovation as reasons that supported its paid priority ban.

Legal Challenges to FCC 2018 "Internet Freedom Order"

- The FCC has statutory duties to consider public safety under its founding act, the Communications Act of 1934 and the Wireless Communication and Public Safety Act of 1999
- The Administrative Procedures Act (APA) imposes a heightened duty to explain changed agency analysis in comparison to the previous proceeding
- Public Safety Concerns were raised in the Internet Freedom Record
- **The FCC failed to analyze the impact of its 2018 net neutrality repeal on critical infrastructure and public safety**
- **FCC Order doesn't consider that repeal leaves remedy only for harms to competition under Antitrust and unfair competition law, and consumer misrepresentation**
- **Arbitrary and capricious decision-making under the APA**
- **FCC proceeding comment process corrupted by Identify Theft, FCC failure to stem identity theft in comment filing**



Democratic Decision-making Process under Threat at the FCC as Criminals use Identity Theft to Argue for Repeal of Rules Protecting the Open Internet




- **Identity theft alleged in FCC "Internet Freedom" proceeding that repealed rules to protect the Open Internet!**

Stolen identities used to file false statements in FCC "Internet Freedom" 2017 proceeding to urge Open Internet rule repeal

- **Professor Sandoval's Reply Comments filed August 2017 support identity theft victim and Congressional demands that the FCC remove the false statements from the FCC web site, investigate, and urge state and federal criminal investigations of alleged crimes perpetrated in the FCC's proceeding, actions**
- **New York Attorney General Schneiderman reported millions of fake comments including 2 million that stole the identities of New Yorkers as of December 2017 .**
- **In 2018 the New York Attorney General and FBI Issued Subpoenas to Investigate the Identity Theft in the FCC's Net Neutrality Comment Process**
- **The FCC's Inspector General agreed in December 2017 to cooperate with the New York Attorney General's investigation. The NY AG Reported that the FCC Chair had been unresponsive and uncooperative**
- **FCC Failure to investigate false comments based on stole identities violates the Administrative Procedures Act (APA) . Woeful neglect of the FCC's duty to the public and threatens democracy!**

Internet Freedom Record Cautioned that Net Neutrality Repeal Risks Public Safety 2016 and on

- **2016 and 2020 Presidential Election cycles increase Internet use for democratic debate and engagement**

- New threats**: Congress finds Russia interfered with U.S. elections in 2016, findings incorporated into** *Countering America's Adversaries Through Sanctions Act* **President Trump signs in 2017**

- **Some interference executed through the Internet by Russians pretending to be people and organizations in the U.S.**

- **Other evidence of hacking including into voter databases**

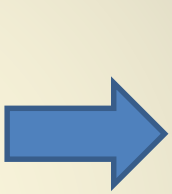
- **Investigations into Russian interference in U.S. elections continue**

- **Oxford University** 2017 report on "***Cyber troops***," "government, military or political party teams committed to manipulating public opinion over social media
- During the 2017 French presidential elections "cyber troops" unleashed bots "to falsely popularize political issues during high-profile campaigns to give the impression of a groundswell of grassroots support"

Gatekeeper Priority Deals Threaten Democracy and National Security

- **ISP Gatekeeper deals can impose costs on and limit avenues for democratic debate**
- **Such deals can also speed messages of those who pay the ISP, influencing democracy**

FCC 2018 Order Eliminates Restraints on ISP Gatekeepers



- Under FCC 2018 Order, Foreign or Domestic entities could buy fast Internet access, even if it degrades other Internet users including critical infrastructure such as energy and water!
- Prioritized accounts are prime targets as they could delay other messages
- Paid priority and the lack of legal enforcement or safeguards puts American national security and democracy at risk!

Videogame vs. the Energy Star

- ISP argued in 2017 in FCC comment that it would like to be able to make paid prioritization arrangement with *video game distributors* for "isolated arrangements," without defining what that is or being subject to regulation.

- **Video Game Pays ISP for Priority**

Vs.

Internet-enabled energy

- **Need to Assess Risks to Critical Infrastructure, Energy Reliability, Safety & the Environment from ISP Paid Priority Deals.**
- **ISP Priority Deals May Degrade Communication to the Energy Ecosystem including Energy Customers and Internet-Enabled Things**
- **FCC places no limits on who, Foreign of Domestic, can buy Paid priority**
- *Who controls the video game*? Interest in Priority or Delay

Videogame vs. Democracy

- If the ISP invokes paid priority while a user in the household or business is playing the video game, or even if the video game's priority is running in the background such as through a sidebar ad, it could delay other signals and messages trying to reach the subscriber or Internet-enabled devices.

- **Video Game Pays ISP for Priority**

Vs.

- **Democracy is not merely voting.**
- **News access and distribution, organizing, sharing through the Internet are increasingly critical to Democratic-Decision-Making**

Democratic Engagement, Decision-making, and Voting

- **These activities influence bills, government decisions, and voting**
- **Paid Priority can be used to interfere with democratic communication**

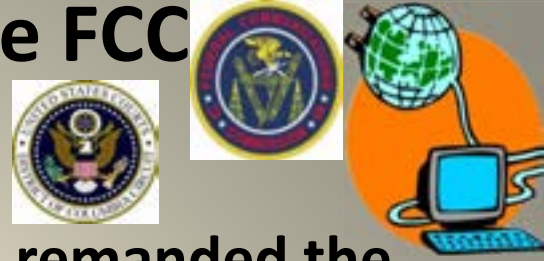
The FCC provides no safeguards for democratic communication

Net Neutrality Repeal Appeal to the D.C. Circuit Court of Appeals

- D.C. Circuit in *Mozilla v. FCC*, 940 F.3d 1 (2019) upheld FCC authority and decision to repeal the regulatory classification that supported Net Neutrality Rules (reclassifying ISPs under Title I of the Communications Act instead of Title II [Verizon v. FCC decided in 2014 held that Title II classification was necessary to impose Net Neutrality rules])

- The D.C. Circuit's decision to uphold the FCC's reclassification of ISPs is on appeal to D.C. Circuit to request rehearing *en banc* (by all of the judges in the D.C. Circuit instead of a panel of 3 judges)(decision pending on this issue

Net Neutrality Repeal Remanded to the FCC for Failure to Consider Public Safety

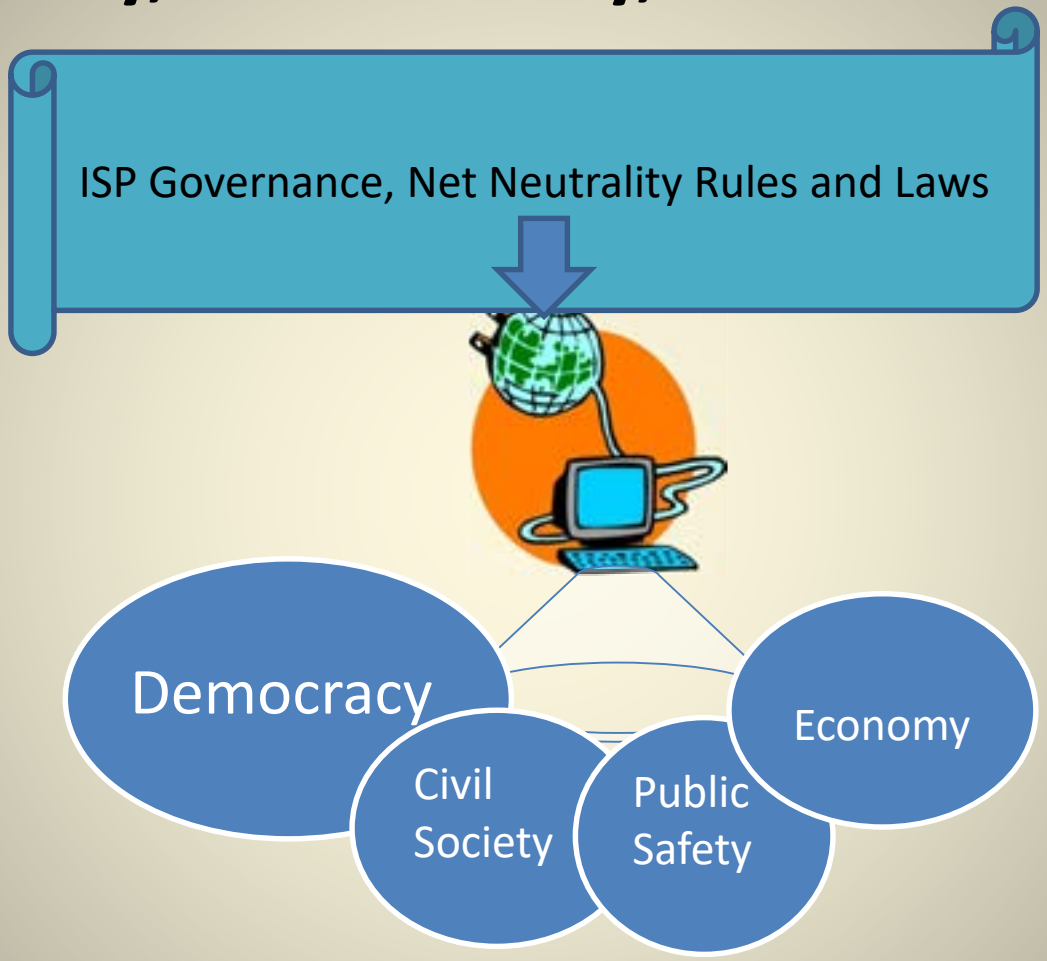


- D.C. Circuit in *Mozilla v. FCC*, 940 F.3d 1, 61 (2019) **remanded the FCC's 2018 Net Neutrality Repeal for failure to analyze or discuss the order's effect on Public Safety**
- The D.C. Circuit emphasized that "the direct and specific comments by Santa Clara County, former California Public Utility Commissioner Sandoval, and others [including the California Public Utilities Commission (CPUC) repeatedly raised substantial concerns about the Commission's failure to undertake the statutorily mandated analysis of the 2018 Order's effect on public safety."
- The CPUC appealed the *Mozilla v. FCC* decision to **only Remand** the FCC order for failure to consider public safety as opposed to **Vacating** the order and also remanding for a new proceeding to consider this issue (appeal is pending)
- The FCC will open a new rulemaking to consider issues remanded public safety and Net Neutrality, likely mid-2020-2021
- *There will be opportunity for public comment on the remand issues, including comment about the appropriate classification of ISPs to address public safety issues raised by net neutrality governance*

FCC Attempt to Preempt State Laws Protecting Net Neutrality Vacated

- *Mozilla v. FCC* Vacated the FCC Order's attempt to Preempt States from Passing and Enforcing Laws to Protect the Internet using State Police Power to Protect Public Welfare and Safety
- California adopted a state law protecting Net Neutrality Law in 2018. California's law is under appeal.
- New York and other states have adopted or are considering net neutrality laws. Some states have adopted laws requiring ISPs observe net neutrality to be eligible for state contracts.
- Under the American federalist system of government, states have the "police power" and duty to protect public safety, public welfare, health, education, etc.
- State net neutrality laws such as California's adopted per state police power recognize the importance of the Internet to public safety, education, health, welfare, transportation, and many sectors that states fund, regulate, or oversee

Internet and ISP Governance Shape Civil Society, Democracy, Public Safety, and the Economy



- *Are Internet Governance and Net Neutrality given sufficient attention and coverage in the U.S. Presidential Campaigns and Debates*?

Thank you!

- Catherine Sandoval, Associate Professor

Santa Clara University School of Law

- Co-Director, Broadband Institute of California
- Co-Director, High Tech Law Institute, SCU Law
- Director, Santa Clara University Summer Law Program at Oxford University

Csandoval@scu.edu

- Please cite this Power Point including graphics to:
- Catherine Sandoval, Digital Civil Society Lab Speaker Series, Stanford University, Feb. 4, 2020