Background Materials:

Whose Law Governs the Metaverse?

Edward McNicholas

ROPES & GRAY

October 2022

AGENDA

- Legal paradigms for the metaverse
- How the U.S. Legal system governs the Internet – or not
- International Organizations
- Soft power: The International Data Protection Consensus
- Data Sovereignty: Building walls

Legal paradigms

Strict Liability	Negligence	Contract	Property
Often based in statute, such as data breach notification laws	Based in private law, as a standard of care	Based on the four corners of the contract	Entitlement to sale, purchase, or use of data
No fault insurance	Industry standards	Law deferential to the terms	Allows for bargaining
Socially-useful but potentially dangerous could trigger liability (i.e., collections of data)	Companies have an incentive to act reasonably to improve compliance and mitigate liability	May limit remedies, damages and set out specific obligations	Activities encouraged consistent with societal recognition of property
Internalization of costs	Evolving questions around standard of care	Reflects bargaining power of parties	Reflects wealth of parties

THE FTC and Section 5 authority

- FTC Act Section 5 prohibits “unfair and deceptive” acts or practices.
- FTC believes an entity can commit an “unfair or deceptive” practice in violation of Section 5 of the FTC Act by virtue of its data practices.

Data Practices are Unfair if:	▪ They are not reasonably calculated to protect privacy or security of consumer information, and ▪ They caused, or are likely to cause, substantial consumer injury that consumers could not have reasonably avoided and that is not outweighed by countervailing benefits.
Data Practices are Deceptive if:	▪ The entity made a material representation or omission regarding information security that is likely to mislead a consumer, acting reasonably, to the consumer’s detriment.
Potential Exposure	▪ Cease and desist order ▪ Ancillary affirmative injunctive relief ▪ Disgorgement/restitution ▪ No penalties (absent order violation)

AGENDA

- The Legal response to cyber attacks
- **How the U.S. Legal system governs the Internet – or not**
- International Organizations
- Soft power: The International Data Protection Consensus
- Data Sovereignty: Building walls

Communications Decency Act

- (1) **Treatment of publisher or speaker.** No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
- (2) **Civil liability.** No provider or user of an interactive computer service shall be held liable on account of—
  - (A)any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
  - (B)any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
- Except:
  - Criminal laws
  - Intellectual Property
  - Communications Privacy
  - Sex Trafficking

U.S. vision for the internet

- “open, interoperable, reliable, and secure internet”
- Department of State (May 31, 2018): Desired end states of U.S. cyber deterrence efforts:
  - “A continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies; and
  - A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force.”
- Clean Network program

Declaration for the Future of the Internet

- protection of human rights and fundamental freedoms
- promotion of a global internet
- inclusive and affordable access
- trust in the digital ecosystem; and
- multistakeholder internet governance.

A DECLARATION *for the* FUTURE *of the* INTERNET

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

RECLAIMING THE PROMISE OF THE INTERNET

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open "network of networks", a single interconnected communications system for all of humanity. The stable and secure operation of the Internet's unique identifier systems have, from the beginning, been governed by a multistakeholder approach to avoid Internet fragmentation, which continues to be an essential part of our vision. For business, entrepreneurs, and the innovation ecosystem as a whole, interconnection promises better access to customers and fairer competition; for artists and creators, new audiences; for everyone, unfettered access to knowledge. With the creation of the Internet came a swell in innovation, vibrant communication, increased cross-border data flows, and market growth—as well as the invention of new digital products and services that now permeate every aspect of our daily lives.

Over the last two decades, however, we have witnessed serious challenges to this vision emerge. Access to the open Internet is limited by some authoritarian governments and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms. State-sponsored or condoned malicious behavior is on the rise, including the spread of disinformation and cybercrimes such as ransomware, affecting the security and the resilience of critical infrastructure while holding at risk vital public and private assets. At the same time, countries have erected firewalls and taken other technical measures, such as Internet shutdowns, to restrict access to journalism, information, and services, in ways that are contrary to international human rights commitments and obligations. Concerted or independent actions of some governments and private actors have sought to abuse the openness of Internet governance and related processes to advance a closed vision. Moreover, the once decentralized Internet economy has become highly concentrated and many people have legitimate concerns about their privacy and the quantity and security of personal data collected and stored online. Online platforms have enabled an increase in the spread of illegal or harmful content that can threaten the safety of individuals and contribute to radicalization and violence. Disinformation and foreign malign activity is used to sow division and conflict between individuals or groups in society, undermining respect for and protection of human rights and democratic institutions.

OUR VISION

We believe we should meet these challenges by working towards a shared vision for the future of the Internet that recommits governments and relevant authorities to defending human rights and fostering equitable economic prosperity. We intend to ensure that the use of digital technologies reinforces, not weakens, democracy and respect for human rights; offers opportunities for innovation in the digital ecosystem, including businesses large and small, and, maintains connections between our societies. We intend to work together to protect and fortify the multistakeholder system of Internet governance and to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet.

We affirm our commitment to promote and sustain an Internet that: is an open, free, global, interoperable, reliable, and secure and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multistakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multistakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition and encourage innovation, promote and protect human rights; and, foster societies where:

- Human rights and fundamental freedoms, and the well-being of all individuals are protected and promoted;
- All can connect to the Internet, no matter where they are located, including through increased access, affordability, and digital skills;
- Individuals and businesses can trust the safety and the confidentiality of the digital technologies they use

Jurisdiction

- Jurisdiction based on various factors
  - Physical location of servers / hardware used to store and transfer data
  - Origin of data or location of consumers or entities whose data is at issue
  - Residence of victims / data subjects
  - Location of individuals accessing data (cloud or integrated intranets)
  - Implications of cross border transfers
- The Conoco-Phillips Candy Store

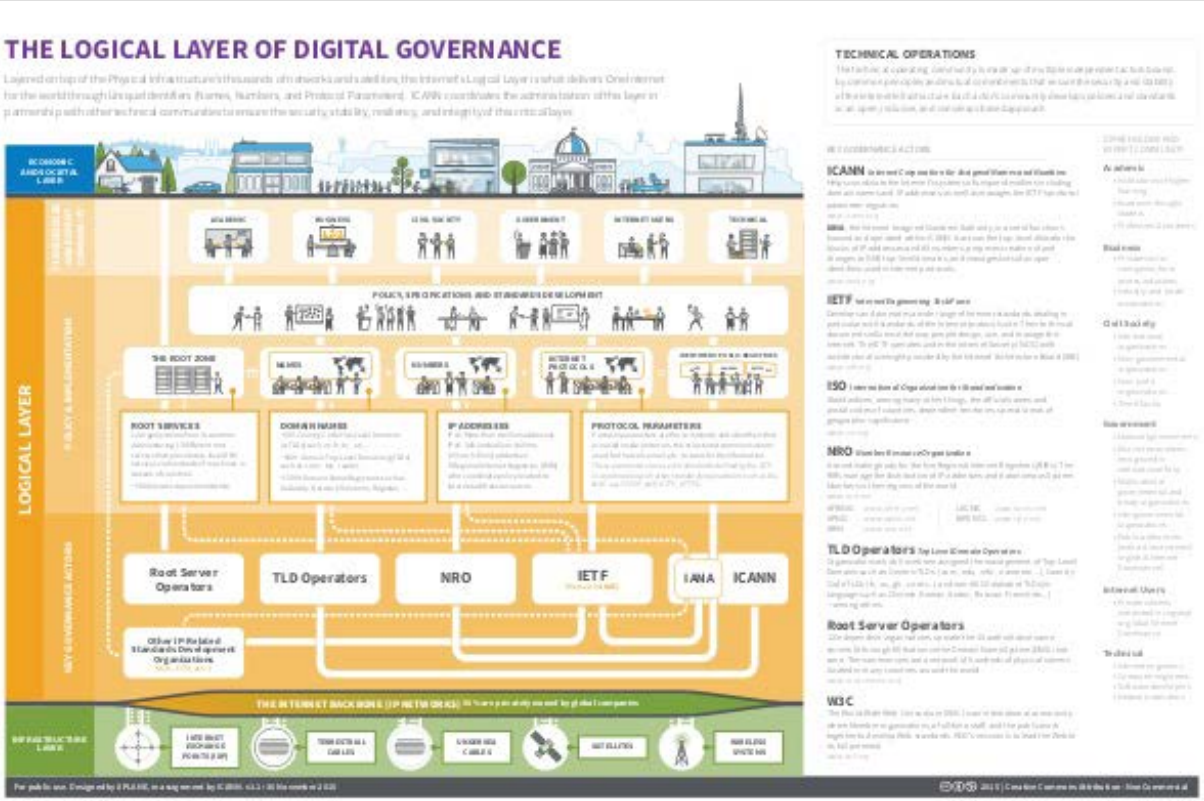
AGENDA

- Legal paradigms for the metaverse
- How the U.S. Legal system governs the Internet – or not
- International Organizations
- Soft power: The International Data Protection Consensus
- Data Sovereignty: Building walls

ICANN

- Internet Corporation for Assigned Names and Numbers handles domain name resolution – globally, without a treaty
- Depends on consensus about which servers are root
- ICANN itself is a nonprofit organized and operating under the laws of California
- Its bylaws are its fundamental law, but those are subject to the control of California and ultimately the U.S.
- Initially, the U.S. gave ICANN a contract to operate the system
- As of October 1, 2016, the functions are under the control of the global "multistakeholder community" which includes international organizations, governments, companies, nonprofits, and interested persons

ICANN's view of its role



ROPES & GRAY

ITU

- International Telecommunication Union is part of the United Nations that focuses on information and communication technologies
- Originally founded in 1865 to promote cooperation among international telegraphy networks, ITU predates many other standardization bodies.
  - Standardization of the use of the Morse code
  - Allocates global radio spectrum
  - Defines satellite orbits
- ITU's global membership includes 193 Member States as well as some 900 companies, universities, and international and regional organizations.

Council of Europe's Cybercrime Convention

- Signatories required to have laws against various computer crimes, including illegal access and interception, data and system interference, misuse of devices, forgery, fraud, child pornography, and intellectual property offenses
- Weak cooperation duties do not work well
- Only the U.S. and roughly 2/3 of the Council of Europe countries have joined

International Information Security Agreement

- Shanghai Cooperation Organization nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan).
- Emphasis on state control and security
- Threat of “dissemination of information harmful to the socio-political systems, spiritual, moral, and cultural environment of the States.”

AGENDA

- Legal paradigms for the metaverse
- How the U.S. Legal system governs the Internet – or not
- International Organizations
- Soft power: The International Data Protection Consensus
- Data Sovereignty: Building walls

EU General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection and privacy regime that tackles a wide range of issues, including how companies must handle their customers' data and what rights individuals have over their own data, including the right of access and the "right to be forgotten".

Network Information Security Directive (NISD)

- Mandates sharing of knowledge on cybersecurity threats and incidents
- Imposes enhanced cybersecurity obligations on “essential service operators” & “digital service providers”
- Requires covered entities to:
  - Continually maintain reasonably adequate security measures to manage cyber risk
  - Report security incidents immediately there is a “substantial impact” on the provision of the operator’s service
  - Implement comprehensive breach notification procedures to comply with NISD reporting obligations stricter than GDPR
- Each Member State to appoint a new regulator and create a new cybersecurity incident response team

EU Digital Markets Act and Digital Services Act

- **Proposal for Digital Services**
  - Amends 2000 e-Commerce Directive
  - Regulates “intermediary services,” e.g., conduit, caching or hosting services
  - Determines obligations and liability with respect to spreading illegal content
  - Systemic risk management requirements for online platforms > 45 million users
  - Additional transparency requirements for online advertising and targeted advertising restrictions
  - Requires very large platforms to appoint compliance officers

- **Proposal for Digital Markets Act**
  - Competition law component of the European Commission’s data strategy
  - Regulates “gatekeepers”
  - Core platform services include online intermediation services, search engines, social networking services, video-sharing platforms and cloud computing services
  - Foresees the creation of a Digital Markets Advisory Committee
  - Currently in trilogue discussions after the council and Parliament each reviewed the commission proposal and adopted their respective negotiating positions

AGENDA

- Legal paradigms for the metaverse
- How the U.S. Legal system governs the Internet – or not
- International Organizations
- Soft power: The International Data Protection Consensus
- Data Sovereignty: Building walls

A Declaration of the Independence of Cyberspace
by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders

Chinese cybersecurity

"Without cybersecurity there is no national security"

President Xi

China’s Ministry of Foreign Affairs

China is a resolute defender of cybersecurity. It advocates for the international community to work together on tackling cybersecurity threats through dialogue on the basis of mutual respect, equality and mutual benefit.

Supply chain safety in cyberspace is an issue of common concern, and **China is also a victim**. China, Russia, and other member states of the Shanghai Cooperation Organization proposed an “International code of conduct for information security” to the United Nations as early as 2011. It included a pledge to ensure the supply chain security of information and communications technology products and services, in order to prevent other states from using their advantages in resources and technologies to undermine the interest of other countries. We hope parties make less gratuitous accusations and suspicions but conduct more constructive talk and collaboration so that we can work together in building a peaceful, safe, open, cooperative and orderly cyberspace.

—Translated by Bloomberg News in Beijing

https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

Not the American vision

Article 12: The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information.

Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

China's Cybersecurity Law

- Law came into force on June 1, 2017
- As early as July 1, 2015, the National Security Law of the People's Republic of China was promulgated, expressly provided that the state shall "safeguard sovereignty and security of cyberspace in the state" -- a key theme
- The Chinese Cyber Security Law strengthens the protection and security of key information infrastructure and Important Data
- Article 21 requires network operators to back up and encrypt Important Data
  - Imposes certain obligations on the "network operators," defined to include owners and administrators of networks, and network service providers
- Article 37 requires operators of "key information infrastructures" to be subject to data localization for personal data and Important Data collected within China

Inspection regulations

- Regulations on cybersecurity supervision and inspections came into effect 1 Nov 2018: “Measures of Internet Security Supervision and Inspection by the Public Security Organs”
- Network operators must provide technical support and assistance to police and national security
- Under the regulation, police may inspect internet service providers, including network operators. Contemplates special inspections during “periods of major national network protective tasks” (Article 12)
- Regulation specifies permissible measures during network security inspections:
  - Physically or remotely enter business sites;
  - Requiring explanations of items under inspection;
  - Reviewing and copying relevant information; and
  - Checking technical security measures. (Art. 14)
- Rules support a sweeping power to inspect companies’ information technology and access proprietary information, perhaps requiring disclosure of source code, encryption keys, & trade secrets

Localization

- Under Article 37 of China's Cybersecurity Law (already effective from Jun. 1, 2017), Critical Information Infrastructure Operators ("CIIOs") are still subject to data localization requirements
- A more wide-ranging data localization requirement was removed from the draft regulation as pertaining to "network operators," but it may be added back into the law
- The localization requirements would make the contents of data subject to access by Chinese law enforcement and intelligence services under Chinese law