INTERNET INFRASTRUCTURE COALITION

Intermediary Liability

Intermediary protections are the key to Internet innovation, and we must fight to preserve them.

Internet infrastructure providers enable people to create and consume content, but it's often agreed that these third parties should not be held responsible for how people use these services. As an analogy, a pen company isn't responsible for what people write or draw with their pens.

Policies attempting to make online intermediaries responsible for all content on their networks are misguided and undermine the Internet's openness and environment. Imparting undue legal risk and regulatory burdens on infrastructure providers impedes their ability to do business and places them in the unenviable position of policing content. A qualified entity such as a court would be best suited to determine what violates a particular law or concept.

Section 230 of the U.S. Communications Decency Act establishes a framework where those responsible for content are liable for their actions, rather than imposing liability on third-party providers. In international trade agreements, we advocate for the sort of intermediary liability protection principles outlined in Section 230.

The safe harbor provisions in Section 512 of the Digital Millennium Copyright Act also fundamentally protect intermediaries from being deluged with contributory liability copyright infringement lawsuits. We support their preservation in order to sustain a proper balance of rights in the copyright law among content creators and online intermediaries.

Privacy

Access to customer information from Internet infrastructure providers should follow the due process of the law.

In some instances, law enforcement agencies have a legitimate need to access personal online data, but government access to data must be preceded by due process procedures set out in the Fourth Amendment in regards to search and seizure. Government information collection is important for matters such as national security and criminal investigations, but for consumers and society, it's important that government access to data follows due process requirements, has a real positive impact on law enforcement activities, and does not undermine consumer confidence in the privacy of data.

Due process protections should exist for the digital world as they do the non-digital one. This would bolster consumer confidence and help ensure the continued positive growth of cloud services. Online activities should be handled with the same privacy protections as in other private communications. Safely storing and retrieving personal data places an enormous technical and administrative burden on this industry to guard against threats from bad actors, and inappropriate state or private industry actions.

On behalf of the Internet ecosystem, the i2Coalition speaks to policymakers and law enforcement agencies both in the U.S. and globally about how privacy and surveillance laws can adhere to due process and protect citizens and their rights online in ways that keep the industry free and profitable.

Encryption

Encryption fosters trust in online interactions. It is a right for Internet users that we must fight to protect it.

Security impacts all Internet users and all Internet service providers. For Internet infrastructure providers, encryption ensures that data flows remain unreadable to unintended recipients such as malicious hackers and government agencies.

Credit cards and personal information leaks due to data breaches regularly make headlines involving compromises that could have been avoided if strong encryption procedures were used. Additionally, many law enforcement agencies and governments have been pushing for

backdoor access to encrypted data, not understanding that built-in security weaknesses could be exploited by bad actors.

Government and businesses need to be educated on the importance of full, end-to-end encryption and its impact on security and privacy.

Digital Trade

The Internet is the world's marketplace. We seek clarity and fairness on how digital trade is conducted, the preservation of open markets, and privacy and trust among consumers.

Global trade meant the exchange of physical goods like steel and lumber for decades, but now more of these goods are digital. Internet infrastructure services have created unparalleled access to goods, information, and services, providing a level playing field for businesses around the world to access global markets.

The Internet is an industry that has succeeded by being administered through self-regulation and market forces. We seek to avoid policies that act as barriers to trade and those that destroy business stability. Uncertainty about liability for third-party content creates a barrier for U.S. Internet companies seeking to compete in foreign markets. It's also crucial to global digital trade to preserve transatlantic data flows that can rationally meet the requirements of privacy law in the U.S. and in other countries such as EU Member States.

Internet Governance

The Internet governance decisions should not be made solely by the US government; The multistakeholder Internet governance model allows Internet users and infrastructure providers to have a say in how it's run.

From its early days, the Internet has been governed on a collaborative basis with constituents sharing ideas and debating best practices. Internet governance has become more complex as

it's grown, but it still follows a collaborative "multi-stakeholder model" where consensus includes representatives from governments, businesses, civil society groups, individuals, and more.

Internet infrastructure provider concerns should be adequately recognized and addressed in multi-stakeholder forums like the meetings of ICANN (a not-for-profit partnership that represents the multiple stakeholders that make up Internet governance). The i2Coalition works to ensure that Internet infrastructure providers' positions are known, understood, and promoted in the ICANN process and in other multistakeholder processes.