CPNI for Digital Platforms

Platforms have both the incentive and ability to exploit user data. In order to compete on a platform, third parties are often required to give sensitive business information they have gathered about their customer to the platform -- data like where their customers are, sales volume, or even profit margins. Platforms can then turn around and use this information to either launch their own competing products or favor chosen products (such as products from those third parties that purchase a bundled service, like delivery). For example, Amazon allegedly used proprietary data from its third-party sellers to launch products under its own label. Even if proven, Amazon's actions would be legal under current law.

A "Customer Proprietary Network Information," or CPNI, regime offers a solution to protect third parties. This concept, borrowed from communications law, defines CPNI as information that relates to the customer's use of a service that is made available to the service solely as a consequence of the customer's relationship with the service.

How would CPNI work for digital platforms?

- The provider that collects CPNI has a general duty to protect their customer's information from disclosure and a set of specific restrictions on the use of information collected.
- CPNI disclosed to the platform or to an affiliate of the platform cannot be used to give an unfair advantage to the platform or for unjust enrichment of the platform. The platform is only permitted to use the data for the purpose it was collected.
- Would apply to all e-commerce platforms as everyone has an incentive to exploit CPNI.
- Rules should be non-waivable by vendors and buyers to protect customer information against dominant platform disclosure.
- Rules would differ for protecting vendor CPNI and buyer CPNI due to the different concerns of both parties.
- All CPNI would be subject to specific exemptions to protect the rights and property of the platform, customer safety, and legitimate search and recommendation functions.
- Enforcement would be through an agency (either new or existing, such as the Federal Trade Commission), as well as a private right of action.

CPNI Is a Targeted Solution

- A CPNI rule would bar certain *uses*, not the *collection* or *storage* of, proprietary business data.
- Examples of acceptable data uses: facilitating the transaction, blocking waste/fraud/abuse on the platform, or using aggregate data to tailor the recommendation functions of a platform.
- Only proprietary business data is protected under the rule. Information readily accessible from other sources like advertisements would not be protected.

- CPNI is a very specific solution to a very specific problem. CPNI should work in tandem with -- and not be seen as a substitute for -- things like a comprehensive privacy law or other competition policies like a non-discrimination rule.

CPNI Has Been Successful in Other Areas and It Can Work Here, Too

- CPNI has its origins in telecommunications, codified as Section 222 of the Telecommunications Act of 1996.
- Used to protect competition in services reliant on interconnection with telephone networks, such as alarm systems or data processing.
- CPNI has been a regulatory success story for the Federal Communications Commission and telecommunications competition.
- The idea behind CPNI can also be found in the financial services industry and insider trading laws.