CENTER FOR DEMOCRACY & TECHNOLOGY

Applying Communications Act Consumer Privacy Protections to Broadband Providers

What is this diagram all about?
With the reclassification of broadband internet access service (BIAS) as a telecommunications service, BIAS providers became subject to the privacy protections of Title II's Section 222. Section 222(c) limits use of customer proprietary network information (CPNI), defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." The FCC will need to interpret how this definition applies to BIAS. One approach would be anchoring the application of CPNI to broadband in the individual components of Internet traffic, known as "packets." Since all Internet traffic is made of packets, a definition of CPNI based on the technical aspects of packets can apply to all transmissions across the Internet.

The accompanying diagram discusses privacy implications of different components of IP packets. Before turning to it, we must answer a few questions:

What is a packet, anyway?
All Internet traffic is divided into packets. Some transmissions fit into a single packet, while longer transmissions are sent in a series of packets. These packets may take different routes through the networks, and may not arrive in the correct order, but the receiving computer can reassemble them if it understands how they are labeled. That's why networked computers rely on protocols.

What are protocols?
When computers sort, send, receive and reassemble packets, they do so according to standardized protocols. These protocols consistently organize the content and routing information so that computers on each end of the communication can understand the meaning of the bytes within the packets' headers (explained below).

What are layers?
Layers are a feature of "network models" of the Internet. The TCP/IP network model is an abstract construct that represents each aspect of an Internet data exchange as a layer. The bottom layer is the actual physical media over which the message will travel, such as copper wire or optical fiber. Above that is the link layer, which describes how the message will be sent across the physical layer. Ethernet and WiFi are protocols that operate at this layer. Above the link layer is the internet layer, which consists of protocols describing how packets will be exchanged across networks. The most common protocol operating here is the Internet Protocol (IP). Above the internet layer is the transport layer, consisting primarily of two protocols: TCP and UDP. This layer determines whether the receiver of a packet needs to send receipt confirmation to the sender and to which part of your operating system the message should be routed. At the top of the stack is the application layer, which contains the actual content of the message such as the file to be read or instructions to perform a task. There are

many application protocols, but one of the most common is the Hypertext Transfer Protocol (HTTP) used to connect users to websites.

What are headers?
Headers are sort of like the shipping information on your snail mail. As your computer sorts information into packets, it wraps the original information with headers. Like information written on a letter's envelope, each of these headers contains data about the data you are sending (metadata) like the size and number of packets in a transmission, where the packet came from and should go, and in what order to open the packets. Just like a mail carrier needs to know your letter's destination, routers within networks across which packets may travel must inspect parts of the packet metadata to correctly forward the packets to their destination. However, neither mail couriers nor ISPs need to know the contents of the letters or packets they transport. When network operators look beyond the packet metadata and into the application data, it is often referred to as "deep packet inspection."

So, what does packet metadata have to do with privacy?
Long-term monitoring of packet headers traveling to and from IP and MAC addresses can reveal patterns and associations that paint a picture of what kinds of information customers are sending and receiving over the Internet, and when, where, and how they do so. For instance, by looking at packet size, packet streams, and IP addresses, a network operator could infer that you are streaming a movie from a particular content provider. A network operator could begin to develop a comprehensive profile of your broadband usage patterns, or even your personal habits, like when you sleep, work, watch movies and send email.

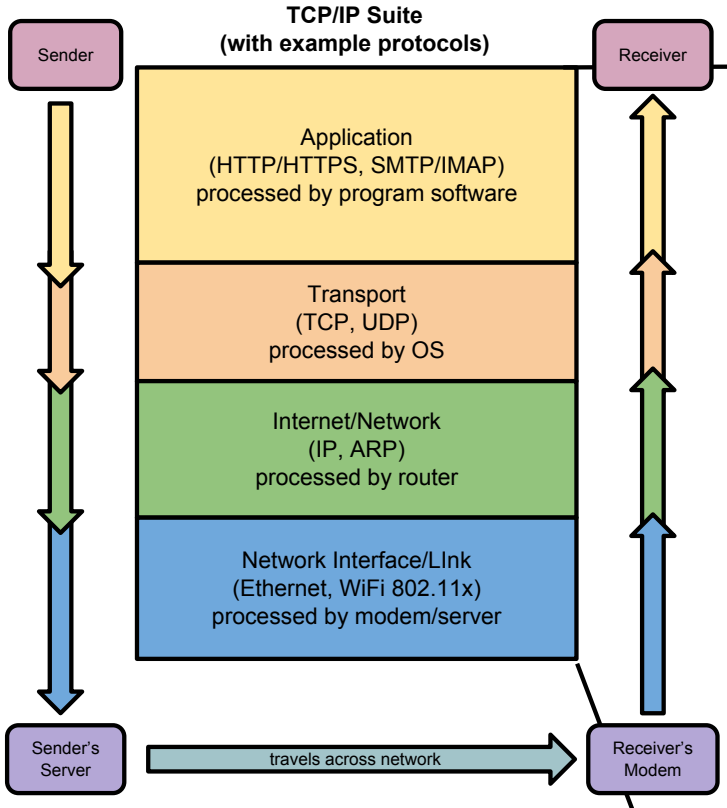
But, what about encryption?
Encryption can enhance privacy, but it is not a panacea. Most encryption occurs at the application layer, meaning the content of a transmission may not be visible to a network operator, but the packet headers are not obscured. If these headers reveal private information, most encryption will not cover it.

Where does that leave us?
Interpreting the definition of CPNI to include packet metadata would not prevent broadband providers from monitoring or collecting header information, but it could limit their ability to market or disclose that information to third parties without customer consent. Some application data may also be considered CPNI, such as the parts of a URL that follow the domain name in your browser's address bar, because this provides even more detailed network location information than the IP header.

The accompanying diagram shows a simplified version of the TCP/IP model on the left, with examples of protocols used at each layer. As a packet of application data moves down through the stack, various components of the application or content provider's computers and network connection hardware add headers to the packet, which then leaves the application provider's server and travels across the

Internet to arrive at your modem. The packet then travels back up the stack, where your network connection hardware remove the headers and deliver the packet payload to your application software.

The right side of the diagram shows an expanded abstract of an Ethernet frame, made up of the application payload and the protocol headers attached to it. The relevant header fields that might be considered CPNI are listed within the packet headers, accompanied by the relevant term from the definition in parentheses. To the right of the expanded packet diagram are descriptions of the potential privacy implications associated with the monitoring and collection of header information.



Customer Proprietary Network Information means information that relates to the ***quantity, technical configuration, type, destination, location, and amount of use*** of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship

Example: Ethernet Frame showing header fields as CPNI			Privacy Implications
Frame Data		Application Data/Content (Encryption)	Application data and content may contain the most private kinds of information, like URLs, ID numbers, purchases, etc. This data would not normally be seen by ISPs unless they perform "deep packet inspection." Ideally, all application data/content would be encrypted, although this is not currently the case.
	IP Packet	TCP UDP Header: Destination/ Source Ports (destination/ location/ type)	Port numbers can indicate what kind of application data is in the payload and may have geographical significance.
		TCP UDP Header: Timestamp (amt. of use)	Timestamps can be used to produce usage patterns, giving clues to other data, like when you're at home (or not).
		TCP UDP Header: Packet Length (quantity/ amount)	Packet length monitoring can produce usage patterns and provide clues about what kind of application data is in the payload.
	IP Header	Destination/ Source IP Addresses (destination/location)	IP addresses can give clues to geo-location, commonly visited sites, and use patterns.
		Total Length (quantity/ amount)	This header field is similar to the Packet Length field in the TCP/UDP header, but shows the length of the enclosed payload plus the header data.
		Type of Service (type or tech config.)	Type of service is not commonly used now, but may gain traction as an indicator of treatment preference, which may serve as a proxy for payload content.
	ARP	Network Protocol Type (type or tech config.)	Protocol type can give clues as to what kinds of data might be in the payload and where, geographically, the sender and receiver may be, particularly when accompanied with hardware addresses.
		Sender/Target Hardware Address (destination/location)	
Frame Header		Destination/ Source MAC Addresses (destination/location)	A persistent, unique device identifier, this data can be used to associate individuals or households with other data points, such as physical location or connection patterns. At home, this is the address of your modem.
			Monitoring a combination of these fields over time can produce a detailed profile of a customer's broadband usage and personal habits.