DOI:10.1145/3281164

Vinton G. Cerf

The Upper Layers of the Internet

The Internet is a layered infrastructure and much has been made of the utility of that layering. IP layer packets are unaware of their underlying transport mechanisms.

The Internet Protocol (IP) layer does not know or care what it carries in its payloads except that they are made up of binary bits. The layer above IP, such as the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Real-Time Protocol (RTP), are equally unaware of the meaning of the bits they carry although they treat these bits differently: TCP keeps packets in order and repairs loss by retransmission. It also filters out duplicates and controls the flow to deal with congestion. The UDP transports packets quickly but without concern for ordering or recovery from loss. RTP uses time stamping and payload typing to cope with jitter and with correct interpretation of the format of the carried bits. Payloads can be marked as audio encoded (for example, G.711, G.723) or video encoded (for example, H.261, MPEG-4), although the meaning of these encoded payloads is opaque to RTP.

Electronic mail is carried in the Internet as Simple Mail Transport Protocol (SMTP). SMTP knows about the format of email messages but not about the meaning of the content. The World Wide Web uses the HyperText Transport Protocol (HTTP) over TCP to carry Web-page content encoded in HyperText Markup Language (HTML). Huge numbers of applications sit on top of HTTP providing useful information or functionality in the form of smartphone or other computing platform applications.

Above these application layers, however, the meaning of the content becomes important. The content of email, Web pages, video and audio streams is

interpreted and used by humans. The transporting protocols and the applications that render content for human consumption are unaware of this meaning. One can imagine, however, a virtual layer above the application layer that deals with content. We might think of this as a political layer, not in the partisan sense, but in the sense that the content is viewed through a policy lens applied by some agreed-upon authority. The operators of application platforms may choose to enforce terms and conditions of use (for example, content inciting violence is not allowed, no one below a certain age is permitted to use the application or consume the content) or may be required by legal means to enforce such restrictions.

Policy is a means of expressing behavioral norms that may also be enforced through law. Policy is a way to provide positive incentive for desired behavior or negative incentive for undesired behavior. In the Internet space, so-called platform providers may self-regulate or may be regulated by external government agencies with the means to compel desired behaviors. The Internet's applications and the providers who support them form a kind of *smart medium* in which content is important. In some regimes, these platform providers are treated as common-carrier-like entities that are not responsible for content while those producing the content are held to enforceable norms. In other regimes, the smart media providers are required to become policers of content at risk of legal sanctions. Incentives for content providers may even

be structured to lead to self-censorship to avoid penalties.

The choices made by governments as to the rules and means by which content is controlled have a profound effect on the nature of the society thus produced. Among the rights expressed in the Universal Declaration of Human Rights is freedom of speech. That freedom may well be abridged through incentives for platform providers either to restrict that freedom or to reveal the identity of the speaker, who then faces the consequences of prohibited speech. In the context of the World Wide Web, in some countries, search engine providers have been required to remove from their indices references to content deemed unacceptable by government authorities. On the other hand, there are endless examples of malware and misinformation that can be seen as harmful speech that threatens the safety and security of citizens and should be filtered and removed.

The permissive openness of the lower layers of the Internet is now plainly challenged by the policy choices made at the virtual political layer. Where lines are drawn in permission space will profoundly affect the utility and ubiquity of the Internet and the society in which it is embedded. The tussle in cyberspace, so aptly named by David D. Clark et al.,^a is far from over.

^a <https://goo.gl/rLYqU8>

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google. He served as ACM president from 2012–2014.

Copyright held by author.