

Geoff Huston

[← Back to Index](#)

Other Formats:  

There is a long-standing role in the communications industry where a provider of public carriage services undertakes the role of a "common carrier". What's so special about the role of a common carrier, and why is this role one that is quite uncommon in the ISP world?

There once was a time when you could not trust the messenger. There once was a time when not only did you pay to have your message sent, but you paid to receive messages. And there was no guarantee that the message would not be read by the messenger. It could be that the contents of your note could be used to determine how much the receiver should pay for the message. It could be that your message was copied and sold to other parties. If you can't trust the messenger then communications becomes a risky business.>

Throughout history the position of a messenger has been a mixed blessing. To be the bearer of bad news was not an enviable role, and rather than being rewarded for the effort of delivering the message, the messenger may well be in dire straits given the level of wrath of the recipient. The option of reading the message before delivering it could be seen as a personal survival strategy, as well as being a prudent business move - bad news could be discarded immediately, while good news could attract the potential of extracting a higher delivery fee from the recipient. Of course while this may be good for the messenger, such a mode of operation was not for the benefit of all. For the parties attempting to use the messenger service, message delivery could be a very haphazard affair. The message may or may not get delivered, the delivery time was variable, as was the cost of delivery, and if the message itself was intended to be a secret, then one could confidently anticipate that this secrecy was going to be compromised by the messenger.

For a communications network to be truly useful there are a number of basic attributes that must be maintained. These include predictability, so that a message passed to a communications carrier is delivered reliably to the intended recipient. Integrity is also necessary, as a message must not be altered by the carrier, nor should the contents of the message be altered by the carrier. Privacy is also an essential attribute, as the message must not be divulged to any other party than the intended recipient, nor should even the existence of the message be made known to any other party. And above all there must be a solid foundation for trust between the carrier and the clients of the service. So in this form of social contract, what does the carrier get in return? Apart from payment for the service, the carrier is absolved from liability regarding the content of the messages, and from the actions of the customers of the service. This form of social contract is the basis for the status of a common carrier.

It may have taken some time, but this role is well understood by the public postal network. And as many national postal operators encompassed the role of national telephone carrier, the common carrier role has been an integral part of the public telephone network.

But in the world of the ISP the position of common carrier is very uncommon indeed.

There once was a time when folk did not need to encrypt their letters nor speak in scrambled code to undertake a private conversation. The assumption, made law in many countries, was that the entity entrusted with public communications, the common carrier, was barred from deliberately inspecting the contents of the plain transmission, and various dire penalties were in place if a public carrier's

employee or agent divulged anything they may have learned by virtue of being a public carrier. Various measures were put in place to execute interception and monitoring, but these measures required due process and reference to some law enforcement agency and also the judiciary to ensure that the rights of the public user were adequately safeguarded.

The issues of the role of a common carrier and the current role of an ISP are clearly seen when looking at the reactions to unsolicited commercial email, or spam. Every day ISPs receive strident demands of the form: "one of your users is sending unsolicited messages - disconnect them now!" Internet users are, in effect, holding the ISP responsible for the actions of its customers. A similar expectation of the ISP's responsibility for the actions of its customers is seen in response to various forms of hacking, such as port scanning. Similar messages are sent to ISPs, demanding the immediate disconnection of those customers who are believed to be originating such malicious attacks. From a small set of complaining messages some years back, the volume of such demands for ISP action is now a clamour that is impossible for any ISP to ignore.

What should the ISP do? Many responsible ISPs see it as appropriate to conduct an investigation in response to such complaints. ISPs often include provisions in their service contracts with their customers to allow them to terminate the service if they believe that their investigation substantiates the complaints on the basis of a breach of contract. Once disconnected, the customer is often blacklisted by the ISP to ensure that the customer cannot return later and continue with their actions. Surely this is an appropriate response to such anti-social actions?

This may be the case, but it is not necessarily consistent with the role of the ISP as a common carrier. A common carrier is not a law enforcement agency, nor is it an agent of the judiciary. It may be entirely appropriate for a common carrier to investigate, under terms of strict privacy, a customer's activities and inspect the contents of traffic passed across the network if it has reasonable grounds to suspect that the integrity of the network itself is under threat. Equally, it is probably inappropriate for a common carrier to extend the scope of such investigations on the basis of external allegations of activities that are not related to the integrity of the service itself.

The assumption that an ISP is, in some way, responsible for the actions of its customers has been extended further in some countries, such that the ISP is, in part, responsible for the content carried over its network, including content that originates with a customer of its service. This expectation that ISPs should actively control and censor content passed across their network is not only an expectation of many Internet users. This expectation appears in a number of legislative measures enacted in a number of countries. The Communications Decency Act in the legislature of the United States is an example of such an expectation of the active role of the ISP in controlling content passed across their networks.

Perhaps the issue here is one of expediency. Where can a user direct a complaint after receiving yet another piece of unsolicited, and possibly highly offensive, email, apart from the ISP of the sender of the message? Where else can the user direct a complaint after being the subject of yet another port scan of their system, but to the ISP? And what else can an ISP do in response? The ISP often has little choice but to investigate such complaints in good faith, and take corrective action if the complaint is substantiated. In the absence of any effective regulatory framework that would allow such investigations to be undertaken by an appropriate external agency, the ISP is in a difficult position. While it may be the correct common carrier position to disclaim all responsibility for the actions of its customers together with the content passed across its network, to ignore such complaints marks the ISP as a haven for such anti-social activities. Adopting such a position often has a negative impact of the ISP's ability to interconnect with other ISPs, as ISPs also tend to hold each other responsible for the actions of their customers and the content passed across their network. ISPs tend to avoid extending interconnection services to those ISPs that disclaim any such responsibility. So the expedient response is for the ISP to assume some level of responsibility for its customers and the network's content and act accordingly.

But short term expedient measures should not be confused with long term effective solutions. The problem with these short term responses lies in the uniquely privileged position of the carrier. Even rudimentary forms of data mining of each customer's communications patterns and the content of their communications can yield vast quantities of valuable information. Such information can allow a carrier to discriminate between customers, compromise the integrity of the customer's use of the network and actively censor the content passed across the network. Positions of privilege without accompanying checks and balances are readily abused. There is already the widespread expectation and acceptance that an ISP has the ability and duty to inspect network content and monitor customer's activities with respect to various form of anti-social and often malicious activities. But how can checks and controls be enforced such that the information gained through such monitoring activities is not used for other purposes? Such monitoring is not without cost, and the option of recouping some revenue to

balance this expenditure by regarding this information as a business asset is always present. The regulatory impost of a common carrier role is intended to be an economically efficient response to this issue. The common carrier role is intended to reduce the social power of public carriers and protect the public's open, uncensored and equal access to the carrier's services.

It is often said that the road to hell is paved with the best of intentions – that the ultimate outcome of the solution is potentially far worse than the immediate problem being addressed. The ultimate outcome of erosion of the common carrier role is that public users of a public communications service can confidently expect their communications to be monitored, potentially stored and cross referenced, and possibly later acted on.

Today the short term expedient measures abound. There is enormous pressure on ISPs from both the Internet's user base and numerous legislatures to take an active position of being responsible, and liable, for the content on the networks and the actions of their clients. If left unchecked this will have severe longer term consequences for free speech, basic personal privacy and uncensored nondiscriminatory universal access to the Internet. And when the user base comes to recognise the debased value of such a compromised communications system they will inevitably look to other means of communication that have retained their essential integrity as a common carriage service.

Perhaps its time for the debate regarding the role and responsibilities of an ISP to be placed on the agenda of public policy makers. Perhaps its time to recognise that ISPs are indeed common carriers and have a clearly bounded set of responsibilities with respect to both content and the actions of clients of the service. Perhaps its time to consider how best to enforce social norms on the Internet without compromising the basic integrity of the carrier as a neutral party to the content being carried across the network. Perhaps its time to recognise that in this domain the Internet is not entirely novel, and what we have learned from a rich history of carriage provision in society has direct relevance to the Internet today.

The Internet is simply too valuable a communications service to have its long term potential as a universal communications service mindlessly sacrificed on the altar of short term expediency.

Disclaimer

I am by profession neither a lawyer nor a public policy maker. However, by virtue of working the ISP industry, I have an increasing level of interest in the activities of these folk, for the reasons outlined above. I should also note that personal opinion comes in many forms. The above is one such form.

The above views do not represent the views of the Internet Society, nor do they represent the views of the author's employer, the Telstra Corporation. They were possibly the opinions of the author at the time of writing this article, but things always change, including the author's opinions!

About the Author

GEOFF HUSTON holds a B.Sc. and a M.Sc. from the Australian National University. He has been closely involved with the development of the Internet for the past decade, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. Huston is currently the Chief Scientist in the Internet area for Telstra. He is also a member of the Internet Architecture Board, and is the Secretary of the APNIC Executive Committee. He was an inaugural Trustee of the Internet Society, and served as Secretary of the Board of Trustees from 1993 until 2001, with a term of service as chair of the Board of Trustees in 1999 – 2000. He is author of *The ISP Survival Guide*, ISBN 0-471-31499-4, *Internet Performance Survival Guide: QoS Strategies for Multiservice Networks*, ISBN 0471-378089, and coauthor of *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*, ISBN 0-471-24358-2, a collaboration with Paul Ferguson. All three books are published by John Wiley & Sons.

E-mail: gjh@telstra.net