Network Neutrality versus Internet Trustworthiness?

FRED B. SCHNEIDER
Associate Editor in Chief

The 1984 breakup of AT&T radically changed the telephone business in the US. More than a quarter-century later, the action has shifted from telephone voice networks to wireless networks and the Internet. Once again, government intervention intended to foster investment and innovation—proposed Network Neutrality restrictions—could radically alter the landscape. Whether the restrictions will have the intended consequences and whether the changes will be good (for individual users, specific commercial users of the Internet, or for society as a whole) is the subject of intense debate. But my concern here is with what's not being debated: how what's being proposed might affect network trustworthiness.

A Network Neutrality requirement would hold that network providers may not block, degrade, or otherwise discriminate against packets based on application or content source. The debate is about whether such a requirement would help or harm innovation and investment in the Internet. Nobody questions that a more trustworthy Internet would be a good thing, and nobody is debating whether Network Neutrality should interfere with that goal. So the various Network Neutrality proposals contain vaguely worded exceptions that do permit network providers, in the name of trustworthiness, to block or degrade traffic within their subnets.

The devil is in the details, and there has been virtually no scrutiny of the details of these trustworthiness exceptions. If the trustworthiness exception is too narrow, it might thwart the deployment of innovative network defenses; if it's too broad, it could become a pretext that protects a wide range of discrimination that Network Neutrality is intended to prevent. Both outcomes would be bad and must be avoided.

For example, in legislation proposed by Senators Byron Dorgan (D.-North Dakota) and Olympia Snowe (R.-Maine), the trustworthiness exception is quite narrow: network providers are limited to offering trust-related services such as spam filtering or virus protection, so long as individual users can opt out of them. This, however, seems to prohibit a network provider from blocking a distributed denial-of-service attack by discriminating against packets destined to, or originating from, a specific set of IP addresses.

As another example, users could benefit if network providers allowed a priori specification of the route taken by packets. This would let users ensure that packets travel only through countries they trust (making it unnecessary to trust the entire Internet); it would also enable users to transmit multiple copies of each packet over independent paths to increase the chances of successful delivery. Yet current Network Neutrality proposals don't prohibit discriminating against traffic on the basis of route preferences.

Other proposed legislation for Network Neutrality allows broader grounds for discrimination. Indeed, some legislation would appear to give providers free rein to discriminate, so long as they can point to a trustworthiness-related reason for doing so. Such a broad exception could seriously undermine neutrality while permitting discrimination with only a nominal connection to trustworthiness.

Additionally, all proposals suffer from a focus on spelling out what network providers, acting independently, can do. The legislation proposed to date thus misses an opportunity to encourage coordinated defenses (though antitrust laws doubtless would place some limits on the kinds of information that providers can share).

Independent of what constitutes a Network Neutrality trustworthiness exception, virtually nothing has been said about how to police its invocation. Network providers are notoriously secretive about peering relationships, so they'll be reluctant to disclose publicly, to their customers, or even to their peers (who would then have details needed to complain about treatment of their traffic) information about traffic and why it was treated as it was. We might imagine requiring network providers to disclose

such information to a regulatory agency (such as the US Federal Communications Commission or Federal Trade Commission), provided the data are exempt from disclosure under the Freedom of Information Act.

This isn't the first time I've written here about interplay between economics, regulation, and system trustworthiness. However, it is the first time I'm writing about a train that hasn't yet left the station. Experts in network security who join the Network Neutrality debate can affect the outcome and increase the chances that the forthcoming legislation will create an economic climate that fosters a more trustworthy Internet.

To have impact, these experts must leave behind their bias about the economic benefits or harms that Network Neutrality per se will bring. They must focus exclusively on shaping trustworthiness exceptions. Ideally, these exceptions would create incentives to deploy defenses we know about today as well as those not yet devised; at a minimum, a Network Neutrality requirement should "do no harm" to trustworthiness. We might start by enumerating the trustworthiness properties customers of the Internet might value. Properties without obvious implementations in endpoints are candidates for implementation inside the network; Network Neutrality legislation should encourage providing such services. Above all, though, we must ensure that any new evolutionary pressures on the Internet select for trustworthiness. ☐

Acknowledgments

This editorial is derived from work done in collaboration with Aaron Burstein. Our forthcoming article in *Federal Communications Law Journal* (vol. 61) gives an expanded treatment of Network Neutrality and Internet trustworthiness.