Network Security as a Public Good

Wendy Seltzer*
World Wide Web Consortium (W3C)
and Berkman Center for Internet & Society at Harvard University
wseltzer@w3.org

Web and Internet security against pervasive monitoring can be characterized as a public good. Like the classic examples of national defense and clean air, a secure and private communication network is non-excludable and non-rivalrous. Moreover, security against traffic analysis on shared infrastructure cannot be wholly self-provisioned; end-to-end encryption between cooperating endpoints can obscure the contents but not the fact of communications between the endpoints. Accordingly, we depend on collective provision of network security, and will often find it under-provisioned if we rely on merely market and individual solutions.

Network infrastructure security exhibits both aspects of a public good. Security is non-excludable, in that while it is possible to create exclusive "more secure" networks, such as VPNs, the very fact of using such a non-public network leaks information: that the communications being sent there are deemed worth extra security or that the user is a member of a class with access to a private network. "Anonymity loves company." Securing the public Internet provides better, more private communications for all its users. Security is also non-rival, even though encryption imposes a per-transaction cost. While network congestion or contention for processor resources for encryption could be identified as individualized costs, overall, these marginal costs are low compared to the costs (both financial and security) that would be incurred in billing for their allocation.

---

* Affiliations listed for identification purposes only. Comments reflect personal position, not that of any institution.

Market solutions to the joint problems of data and metadata security remain elusive.

Because individual participants cannot fully capture the benefits tied to the costs of public goods provisioning, a pure market environment will tend to under-supply public goods. Thus we still see a great deal of unencrypted traffic on the Internet, even as individuals and businesses increasingly encrypt their own data. One common response to public goods challenges is government provision, yet in the Internet security context, government has emerged as one of the threats. Even those not concerned by their governments' ability to surveil their communications are jeopardized by the modes of such surveillance: government agencies' deliberate creation of back-doors and concealment of known bugs weaken security against non-government actors as well.

Perhaps all is not lost. Collectively, participants in the Internet ecosystem can both recognize the nature of the problem and take steps to manage the environmental challenges. If we recognize the shared risks of information insecurity – and our inability to mitigate these risks individually, we can work to address them in Internet institutions such as IETF and W3C, as stewards of a network security commons. These institutions require checks and balances, open and fair processes, and the cooperation of participants with divergent interests, but the common good of network security depends on our making them work.