The Privacy Risks of ISPs Using Deep Packet Inspection

by Alissa Cooper [1]
July 1, 2010

Deep packet inspection (DPI) -- technology that potentially allows providers of Internet service to collect and analyze the Internet communications of millions of users simultaneously -- has been a hot topic in a number of different policy circles in recent years. In the privacy arena, ISPs' use of DPI has drawn scathing criticism despite the fact that other kinds of service providers (like content delivery networks and web-based service providers) are capable of conducting content inspection. In a guest essay over at the Canadian DPI portal DeepPacketInspection.ca [2], I explore what separates ISPs from other kinds of service providers, and why their use of DPI can raise unique concerns:

> There are several characteristics inherent to ISPs and their use of DPI that significantly increase the privacy stakes as compared to these other entities . . .. ISPs are uniquely situated in three respects: they serve as gateways to all Internet content, switching ISPs can be difficult for Internet users, and their use of a tool as powerful and versatile as DPI makes it prone to mission creep. An exploration of each of these factors reveals that they are difficult or impossible to mitigate. Taken together they form the fundamental basis for the heightened privacy alarm that has characterized DPI debates.

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://www.cdt.org/blogs/alissa-cooper/privacy-risks-isps-using-deep-packet-inspection

Links:
[1] https://www.cdt.org/personnel/alissa-cooper
[2] http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/