A user might typically want to use such proxies for only some of their activities (say to follow the news surrounding anti-government protests), while still enjoying "un-handicapped" Internet for other activities (such as watching full HD cat movies).

The problem with such an approach, again, is that the potential malware might choose to piggyback the stolen information onto the innocent traffic.

About the only one left solution here would be to keep an eye on the traffic generated by the user. The adversary knowing that the user might be closely monitoring their traffic should be reluctant to (somehow blindly) piggyback a covert channel on top of it, afraid of getting caught. Thus, it would seem more reasonable for the adversary to target higher-level protocols also in this scenario, facing also the same problems as discussed in the previous section.