The do-not-track issue is in the middle of two very different, very conflicting interests. While many end users are concerned about being tracked without their knowledge, content providers want (and increasingly depend on) revenues associated with targeted and behavioral advertising. In addition, governments and software vendors have entered the dispute, proposing regulation and implementing HTTP headers to give users the ability to opt out of tracking. However, both solutions by themselves have issues. Trackers could simply ignore do-not-track headers. Regulators could outright ban tracking, which would damage the current model supporting free content through online advertising, or they could set up a Do-Not-Track registry, which would be far more difficult to accomplish with online identities than the Do-Not-Call registry was for static phone numbers, not to mention it would be prone to loopholes. I propose a hybrid solution in which consumers may individually weigh the tradeoffs between privacy and access to free content.

One fundamental component of this hybrid system is the user's right to privacy. That is, the user should have the option to not be tracked without any direct financial cost. I would implement this as the proposed opt-out do-not-track HTTP header. Of course, content providers have the right to be compensated for producing content (if only to cover the costs of producing it), so it would be perfectly valid for a provider to restrict content to those users who do not send the header. This could evolve into a two-tiered system where users either forfeit their privacy in order to access content for free or pay a premium to not be tracked. The user who sends the do-not-track header while still expecting to see content without the premium is bound to be disappointed, but he or she is not necessarily entitled to something for nothing.

However, the user should be allowed some baseline privacy rights even in this "free-with-tracking" tier. Since it would make sense in such a two-tiered system for the default browser settings to not send the do-not-track header (as otherwise the Internet could be a small, closed-off place for the non-tech-savvy), the average user needs some basic protections to prevent being exploited. The authors of such protections could start with banning the obvious — drive-by spyware downloads, external site viewers that bypass browser security, etc. The protections could be amended as needed, to prevent tracking companies from abusing technologies that do not yet exist.

Of course, content providers could just choose to ignore all this without regulatory enforcement. Much of what would go into the baseline privacy rights are already covered through existing laws. However, regulators would also need to require that content providers respect the do-not-track header upfront as well as provide some sort of mode (even if it requires a premium) that respects the header without impacting usability of the website. Such regulations could be part of the many-times-proposed Internet Bill of Rights. Of course, there would have to be provisions defining both when usability becomes negatively impacted and when a premium becomes extortionate, but the latter at the very

least might be solved by the market and/or monopoly law.

While consumer and content provider interests seem to be at odds, it is possible to develop a system that is fair to everyone. Such a system must combine both technological and regulatory solutions to actually be effective. While the content provider and advertising companies are not entitled to exploit end users, end users are not entitled to get something for nothing either. This is just one possible proposal that can balance the interests of both groups.