# Third Party Apps: The Role of the Developers vs. The Role of the Platform in Protecting Security and Privacy – Ari Schwartz

The past two years have seen the introduction and rapid adoption of a new model for online services: companies are increasingly opening their platforms to the public, allowing every-man innovators, advertisers, and even competitor companies to contribute applications that enhance the original platform in previously unimaginable ways. In inviting unknown third parties to develop extensions to their carefully developed platforms and well-honed brands, these platform providers have taken on an ambitious task: promoting a vibrant, open marketplace while striving to maintain a secure online environment and retaining consumer confidence in that environment. Efforts toward these desirable, but at times seemingly contradictory, goals have met with varying levels of success. In some cases, companies have even created new economic ecosystems within these platforms.

Companies that are considering opening their platforms must all confront a set of key questions: how involved will they be in vetting applications designed by third parties for their platforms? What types of guarantees – if any – do they want to make to consumers about the security of applications offered in their application "stores"? How can they protect users from applications that enable fraud, identity theft, privacy violations, and security breaches and thereby protect their brand? By making guarantees about these third party applications, are they opening themselves up to liability if seemingly innocent applications are in fact nefarious?

Liability issues for these applications are not entirely dissimilar to liability issues on the Web or the Internet as a whole. As with the other areas, the threat of liability inhibits the willingness of intermediaries to host user-generated content; such liability leads intermediaries to block even legal content and could inhibit innovation. Individual users should be held responsible for their unlawful actions, but if the threat of liability discourages Internet intermediaries from allowing users to communicate in the first place, then the opportunities for even lawful expression will be curtailed and the potential of networked technologies will be diminished.

Governments can play a proactive role without impinging on innovation in this space in two important ways:

1) Aggressively pursuing applications that violate privacy and security laws. It is the application itself and not the platform that hosts the application that must ultimately be held responsible for breaking laws regarding the security and data protection of personal information.

2) Encouraging companies to offer consumers tools to protect themselves and defending companies that offer such tools. Anti-virus and anti-spyware companies have been a vital means of defense for consumers. Makers of security software should be encouraged to root out bad applications and platforms should be encouraged to provide users with security and privacy enabling tools. Governments can offer these companies liability protection when researching, alerting and disabling applications that may impinge on safety, security and privacy.