Privacy and Data Security

Whereas,

Digital technologies and online communications have created extraordinary business opportunities for Apple; they may also present serious risks to privacy and data security.

Breaches of privacy and data security are a constant threat which can result from either company negligence or external attacks. Cyber attacks on U.S. computer networks rose 17-fold from 2009 to 2011, according to the U.S. National Security Agency, with many companies not even realizing they were attacked. Privacy breaches have also grown dramatically in recent years.

According to a 2011 Ponemon Institute study, the per capita cost of a data breach was $194, with an average incident cost of $5.5 million. Further, a separate Ponemon study found data breaches could negatively impact brand value and reputation by as much as 17 percent to 31 percent, with the average loss in brand value ranging from $184 million to more than $330 million.

Unauthorized collection, disclosure, or misuse of personal information can cause great harm to individuals and society - including discrimination, identity theft, financial loss, loss of business or employment opportunities, humiliation, reputational damage, questionable government surveillance or physical harm.

We believe Apple's Board has a fiduciary and social responsibility to protect company assets which include the personal information of a variety of stakeholders.

Recently, Apple confronted a number of cyber security and privacy controversies - drawing the attention of Congress and groups like the ACLU. The controversies include unauthorized access to iPhone users' address books; Unique Device ID related litigation and the release of one million UDIDs; and security concerns related to iCloud. We are concerned future controversies and litigation could place critical growth opportunities such as iCloud at risk.

Resolved, that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

Supporting Statement

It should be emphasized that the Proposal is not asking the Company to disclose risks, specific incidents, supplier relationships or legal compliance procedures, but rather, we believe investors need to understand more fully how the Board is overseeing the concerns described above.

Carnegie Mellon University's Cylab published a 2012 report ("How Boards and Senior Executives Are Managing Cyber Risks") which we believe could be instructional in writing this report. Among Cylab's recommendations for boards:

- "Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility."

- "Review assessments of the organization’s security program and ensure that it comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans."

- “Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.”

- "Require regular reports from senior management on privacy and security risks."