Shareholder Proposal: Spy Lockout

November 29, 2013 David Levitt, Apple Shareholder

General Counsel Bruce Sewell
Apple Inc.

Re: Advance Notice of Shareholder Business

Dear Mr. Sewell,

… Over the course of 2013, new information regarding the relationship between government surveillance and private corporations have impacted Apple's public image in ways that concern me as an investor. I hope you understand this is not a frivolous or unique interest of mine, but one that is shared by many other shareholders. We are deeply concerned by Apple's failure to publicly renounce and take all necessary steps to prevent these violations. Some shareholders have already retreated from their prior stake in Apple.

Courts have already ruled (at times secretly) that misrepresentation and over-collection of data by government agencies has been ongoing. Court orders and warrants requiring Internet Service Providers to enable violations of all their users' privacy are issued, in secret, with gag orders. SSL security keys are compromised, stolen, or coerced from executives and engineers.

Meanwhile, as of 5 November 2013, Apple has vowed maximum transparency within the law. We commend Apple's new approach and welcome this significant progress.

But thus far Apple has declined to say definitively whether it has already received court orders that, for example, allow equipment to be installed at Apple premises that might be in use by bulk surveillance programs – putting up to 350 million iCloud users' data in jeopardy. In this context it is reasonable to conclude that governments have already requested such cooperation from Apple, under gag order, holding Apple staff and/or executives hostage.

This crisis of trust in US companies has already seriously injured international technology firms like Cisco.

Resolving this cannot wait another quarter – let alone another year – without serious injury to Apple. We wish to present this issue, and we welcome alternatives put forward by Apple that might help effectively resolve these threats to customer and investor confidence.

In the event there is insufficient response by Apple, we will submit a proxy shareholder proposal that may compel Apple to act belatedly in 2015.

Please contact me as soon as possible if you have any questions or concerns. I look forward to attending the Annual Meeting to raise this issue.

Shareholder Proposal: Spy Lockout

Apple has approved the following proposal for discussion at its February 27, 2014 shareholder meeting in Cupertino. The shareholder who raised it, David Levitt, will be given 2 minutes to speak. A non-binding vote will be held of shareholders present. More important, we expect Apple to answer and implement the proposal without waiting for a binding order from stockholders, to prevent the continuation of serious long-term harm to the company.

Resolved:

A group of concerned Apple shareholders proposes several technical and policy actions Apple should take immediately, without waiting to be compelled by shareholders, to quickly earn back user trust and demonstrate Apple's competence in repelling modern threats to user privacy.

We ask that the board enact a policy to use technical methods and other best practices to protect user data. Such best practices include:

- Encryption: Implement encryption techniques such as Forward Secrecy and the other recommended best practices cited in the Electronic Frontier Foundation's recent reports on encryption.
- SSL Key Revocation: Revoke and update SSL encryption keys and any similar digital entities that may have been compromised, immediately and as often as necessary for the security of user data.
- Secure Network Equipment: Remove or replace any equipment that may be used for unconstitutional bulk surveillance at sites managed by Apple, to every legally permissible extent. Third-party equipment, such as interception devices installed in compliance with "pen trap and trace" orders, should provide access to confirm the devices can not be used for unconstitutional bulk collection or over-collection of data. If any court order or warrant must be withdrawn or revised to achieve this, Apple may seek relief from the courts – such as FISC courts that have already discovered systematic over-collection of data and ruled some programs unconstitutional – in the course of legally removing such equipment.
- Transparency: Expand deployment of measures such as the "warrant canary" and "dead man switch" so users can be confident that Apple networks and encryption keys have not been compromised – or can be alerted if they are.

Moreover, as a U.S. company Apple has constitutional and ethical duties that include respecting the 4th Amendment.

Apple should, to the full extent permissible by law, deploy its strengths in both technology and law to publicly reveal, challenge, reduce, and overturn every government attempt at covert surveillance against its customers that doesn't meet these standards: surveillance of single, identified individuals under a warrant issued by a neutral judge, particularly describing the person and places to be searched, and of limited duration. To the full extent permissible by law, Apple should not actively or passively agree to do or allow covert mass surveillance against its customers, nor remain silent about what Apple and the government have done or are doing.

Lost trust will not be regained until Apple users and shareholders understand whether Apple is a paid participant in unconstitutional bulk surveillance, a hapless victim of it, a gagged hostage of government spies, badly in need of help – or, whether Apple is truly an effective foe of such surveillance.

For stewards of user data like Apple, both ethical standards and user trust are essential to sustaining shareholder value. Failing to acknowledge and address these realities can cause the company serious ongoing financial harm, particularly in international markets. Conversely, by addressing these issues forthrightly Apple can win back the trust of customers, provide leadership, offer competitive advantages, and strengthen the entire industry.