Microsoft

Microsoft New Zealand Limited
Auckland, Wellington, Christchurch

For the Members
Law and Order Select Committee
Parliament

20 June 2013

Microsoft New Zealand Limited appreciates the opportunity to comment on the Telecommunications (Interception Capability and Security) Bill.

We are a wholly-owned subsidiary of Microsoft Corporation, which is headquartered in the United States and offers devices, products, services, and software that are distributed to individuals, businesses, governments, and other organisations.

We recognize the important balance that must be struck between human rights including privacy, innovation, law enforcement, and national security.

Microsoft published an inaugural Law Enforcement Requests Report in March 2012 at http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/. The report reflects, among other information, the company's commitment to the rule of law, and the company's policies and disclosures in response to law enforcement requests, including those from New Zealand.

The draft legislation in New Zealand clearly strives for balance. However, we submit that the current draft is in need of substantial work if the legislation is to reflect the reality of today's technology and global flows of information.

The stated purpose of the legislation in clause 5 is that the interception assistance should not "create barriers to the introduction of new or innovative technology" and that there should be the "freedom to choose system design features and specifications that are appropriate".

We submit that, as currently drafted, Part 2 Subpart 5 of the Bill will not meet these objectives for the reasons set out below.

Technology providers could face conflicting obligations. Part 2 Subpart 5 could, with little prior warning, place technology providers in a position where New Zealand law puts them in conflict with pre-existing obligations that they have under overseas laws. Technology providers will be placed in an invidious position if they are forced to choose which country's laws to break, or discontinue a service.

Uncertainty could reduce access to new innovations in New Zealand. It is unclear which technology providers (if any) will become subject to the obligations under Part 2 Subpart 5 in the future, but it is clear that many technology providers will be *at risk* of having to meet these new obligations for any or all of their telecommunications services that they provide in New Zealand, at

very little notice. In those circumstances, it is not difficult to see that technology providers will be more reluctant to invest in building new services in New Zealand or deploying them in New Zealand. Technology providers will be unable to plan for interception capability obligations with any certainty when building services, and there is no indication in the Bill that technology providers would be compensated by the Government for the additional costs of retro-fitting interception capabilities into pre-existing services.

Interception capabilities may not be technically feasible. It is not technically feasible for all technology providers (or network operators) to offer an interception capabilities for all telecommunications services. For example, technology providers have no way to know the content of communications that occur directly between the individuals concerned. Technology that enables direct communications (also known as peer to peer) between individuals is commonplace. Part 2 Subpart 5 does not expressly contemplate that technical feasibility needs to be considered by the Minister.

The Bill could lead to discriminatory penalisation of individual technology providers. Part 2 Subpart 5 contemplates that decisions could be made that discriminate against individual technology providers by imposing unique legal obligations or restrictions on them, even where they have not breached any New Zealand law. Any unequal treatment of similarly-situated technology providers has the potential to be unfair and discriminatory, and could have negative consequences including distorting competition, stifling innovation, and arbitrarily depriving people of socially and economically beneficial technology.

The Bill could lead to dramatic extensions to the scope of surveillance agency oversight without Parliamentary oversight. Part 2 Subpart 5 will allow executive Ministerial decisions without any direct public or Parliamentary oversight to extend the scope of organisations that are required to be intercept ready or intercept accessible. That has the potential to widen the scope and of surveillance agency access and oversight over New Zealand citizens. Microsoft submits that all decisions to extend obligations to be intercept ready and intercept accessible to additional organisations or classes of organisations should be made openly by Parliament, not by an individual Minister.

Relevant considerations are too narrowly constrained by the Bill. Part 2 Subpart 5 proposes to limit the Minister's discretion to strike the right balance on these important matters. Clause 35(8) obliges the Minister to give "primacy" to only one of the many important factors that should be properly be weighed up. The factor that must be given primacy is "whether the current level of interception capability on any services provided by the affected service provider adversely affects national security or law enforcement". Arguably, this could almost always be answered in the affirmative. In other words, it appears that the Minister could almost always say "yes" to new duties to be intercept ready and intercept accessible. It could even be difficult for the Minister to defend a judicial review initiated by the surveillance agency if the Minister declines.

Part 2 Subpart 5 does not ensure adequate time for response. There is no assurance in the Bill that technology providers will have adequate time to prepare submissions to the Minister if they are faced with a decision under Part 2 Subpart 5 that could have a dramatic, unpredictable, sudden, and far-reaching impact on their business and all of the telecommunications services that

they provide to New Zealanders. Given the highly technical nature of the subject matter and the far reaching implications of decisions, we submit that if Part 2 Subpart 2 is retained, technology providers should be assured of adequate time to prepare submissions and complete other processes that may be required.

Law enforcement in the context of international services is a complex area that can only have a satisfactory solution if it is resolved consistently on a multilateral basis and with full knowledge and understanding of the technology. New technologies that function globally across multiple jurisdictions could be significantly constrained by inconsistent border-based laws. We encourage New Zealand to be thoughtful in developing an approach that is interoperable with other nations, and to seek to find the right balance in cooperation with other sovereign nations rather than working alone.

We look forward to contributing to the discussion on this topic as New Zealand contemplates new legislation. We hope to contribute, among others, to legislation that will meet New Zealand and the global community's need for growth and connectivity.

We would like to request an appearance before the committee to speak to our submission.

Yours sincerely,

Waldo Kuipers
Corporate Affairs Manager
Microsoft New Zealand Limited