facebook

7 July 2012

For the Members
Law and Order Select Committee
Parliament

Re: *Telecommunications (Interception Capability and Security) Bill*

Dear Committee Members:

Facebook welcomes the opportunity to provide comments on the *Telecommunications (Interception Capability and Security) Bill* (**the Bill**). We thank the Committee for an extension to file this submission.

Facebook's mission is to make the world more open and connected. Over 1 billion people are using Facebook on a regular basis across the globe, including over 2 million people in New Zealand. Each month, Facebook enables every one of these users to share information – photos, status updates, and private messages – with their friends.

In summary, we believe that the Committee should recommend that the Bill be clarified and narrowed in scope. Firstly, the Committee should ensure that there is no potential for confusion that stored messaging services such as those provided by Facebook could be interpreted as being within the remit of the Bill. Secondly, we encourage the Committee to take account of five important principles in narrowing the scope of this Bill to ensure that the proper balance is struck between user privacy, on the one hand, and national security and law enforcement interests, on the other. These principles are that any procedure be structured to give regard to: proportionality; due process; efficiency and cost; the need for transparency; and, with regard to jurisdictional concerns.

The uncertain scope of the current Bill and proposed structure has the potential to stifle the delivery of and development of innovative services in New Zealand and will potentially create regulatory environment with which compliance is not technically and legally possible. As such, Facebook submits that, as currently drafted, the Bill would not meet the stated purpose in clause 5 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".

Facebook Policies

Before we turning to the details of our concern, we thought it may be useful to provide some background information about Facebook's policies and procedures.

We respond to requests from law enforcement authorities around the world according to our terms of use and applicable law. We have established processes for law enforcement authorities to submit requests and these are set out in published Law Enforcement Guidelines to provide operational guidelines for law enforcement officers seeking records from Facebook.[1]

In order to ensure that our processes are well understood, Facebook security representatives have provided workshops for New Zealand police officers. The New Zealand law enforcement authorities are therefore very familiar with these voluntary processes and make good use of them.

We respond expeditiously to New Zealand law enforcement requests, making sure that we prioritize any cases where there is an imminent risk of death or bodily harm.

In certain cases, a request may only be fulfilled by using the Mutual Legal Assistance Treaty (MLAT) process, which permits the New Zealand government to make a formal request of the US government to obtain evidence maintained in the United States.

Our Statement of Rights and Responsibilities[2] and our Data Use Policy[3] underpin Facebook's relationship with its users. These policies prohibit the use of our services for illegal activity. Unfortunately, just as there are offline, there are occasions when people misuse our services and jeopardise the safe experience our users. Our goal is to respect the balance between law enforcement's need for information and the privacy rights of the people who use our site. We realise this goal through rigorous policies and procedures.

We undertake numerous activities to ensure users understand these policies and are able to make use of the controls we provide for them. There is a comprehensive online Help Centre[4] and an extensive User Operations function operating 24 hours a day via four locations around the globe.[5]

Specific comments

Our specific comments on the Bill are that it needs to be clarified to ensure that it is beyond doubt that services such as Facebook that provide stored messaging services are not subject to this legislation. In addition, we believe that the Committee should narrow the provisions contemplated by the Bill mindful of the principles we outline below.

Firstly, as presently drafted, we are concerned that the Bill could potentially be interpreted to require Facebook to provide an interception capability. The Bill requires in Part 2, Subpart 1, Section 9 that "public telecommunications networks" that are provided in New Zealand have full interception

[1] https://www.facebook.com/safety/groups/law/guidelines/
[2] https://www.facebook.com/legal/terms
[3] https://www.facebook.com/about/privacy
[4] https://www.facebook.com/help/?ref=pf
[5] More information about our user operations team is provided in this note to the Facebook Safety Page: https://www.facebook.com/fbsafety/posts/331112966969938

capability. "Public telecommunications network" is, in turn, defined to include a "public data network" which includes services data networks that provide email access.

Facebook recommends that the Committee clarify this to ensure that it is not intended to apply social platforms that also provide stored messaging facilities such as Facebook.

We believe that law enforcement should have effective methods to address crime that are proportional to the impact on citizens and companies. We believe that narrow, targeted, proportional rules should always be preferred over blanket rules requiring interception and accessibility. Blanket rules requiring data retention and accessibility are blunt tools, which have the potential to infringe on civil liberties and constrain economic growth.

Secondly, in our view, the Committee should shape any recommendations with respect to lawful access against the following principles:

1. **Proportionality**: Users enjoy privacy rights and have a legitimate expectation of privacy for the data they share online. Accordingly, provisions that empower law enforcement to obtain lawful access to user data held by service providers must be limited in both time and scope to focus on particularised information relevant to a criminal investigation.

2. **Due Process:** Service providers should be required to disclose account content and communications only by a search warrant or other court or tribunal process that has been issued based on meeting the standard of probable cause as assessed by a judge or equivalent public official.

   Further, targeted and proportionate investigation of criminal offenses is available to New Zealand law enforcement through appropriately authorized judicial warrants or international standards like the Mutual Legal Assistance Treaties (MLAT) that the New Zealand Government has entered in to with various different foreign governments. This international standardised process allows a court or judge to ensure proportionality of each request is tested before data is accessed.

3 **Efficiency and Cost:** any process should be structured in such a way as to ensure that appropriate checks are placed on the over-use of orders.

   For example, laws granting lawful access should impose the costs of fulfilling those requests on the law enforcement authorities that request the information, and not directly or indirectly on service users. Financial constraints can serve to place an institutional check on the over-use of orders.

   In addition, appropriate time should be allowed for service providers to challenge decisions under the Bill. At present, Facebook is concerned that Part 2 Subpart 5 does not ensure adequate time for response. There is no assurance in the Bill that online service 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. We encourage the Committee to ensure that more time is allowed for responses.

4. **Transparency:** Law enforcement agencies should publicly provide citizens with the full information they need to exercise their democratic right to hold agencies accountable for when and why they issue demands to online service providers for user information.

   As presently drafted, the Bill could lead to an extension 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. Facebook encourages the Committee to propose amendments to this Bill to ensure 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.

5. **Jurisdiction:** Domestic legislation should account for existing legal obligations on providers that arise from the jurisdictions where data is stored and controlled and avoid imposing mutually exclusive or conflicting requirements.

   This principle of jurisdiction is informed by the fact that online companies offer services accessed via the Internet across the globe. Consequently, we face the real prospect of many different governments identifying new national legislation on lawful access as the means to achieve security objectives in respect of services like ours.

   We are concerned about the potential for a chaotic situation of conflicting legal requirements and overlapping jurisdictions for and against disclosure in different countries (countries where the data are stored, or where the law enforcement authorities are based, where the users of the service are located or where the personal data are controlled, etc.). Were this situation allowed to develop, it must be likely that law enforcement will be impaired rather than enhanced in New Zealand and across the globe. In particular, Part 2 Subpart 5 could put online service providers such as Facebook in a position where New Zealand law puts them in conflict with pre-existing obligations that we have under overseas laws. We therefore believe that it makes more sense to sustain and where necessary reform existing models of cooperation within uncontested jurisdictional boundaries.

We thank the Committee for the opportunity to contribute to this process.

Kind regards,

Mia Garlick
Head of Policy
Facebook, Australia & New Zealand