Privacy Officer, Legal Department
Tencent
Level 29
Three Pacific Place
1 Queen's Road East
Wanchai
Hong Kong

March 17, 2016

Dear Madam or Sir,

Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, is currently researching the security and privacy features of QQ Browser (Android and Windows versions). On February 5, 2016, we used the Tencent Security Response Center to notify Tencent of security vulnerabilities we discovered in the browser. We write now concerning broader issues of user privacy and access to information implicated in the browser's design.

Our research findings raise the following questions for Tencent, to which we would appreciate your timely response:

1. QQ Browser (Android version 6.3.01920 and Windows version 9.2.5478) collects detailed and extensive user data, including user and hardware identifiers as well as search queries, as documented in our security disclosure. For what purpose is the user data collected and utilized? Is Tencent required to collect such information pursuant to law, regulation, or policy (internal or external)? If so, which laws, regulations, or policies?

2. For how long does Tencent retain the user data that it collects through QQ Browser? How is that data stored, and what security measures are in place to protect that data at rest?

3. Does Tencent share the user data it collects through QQ Browser, and if so, with whom?

4. What if any laws, regulations, industry standards, or policies (internal or external) guide Tencent's approach to the use of encryption in transmitting or storing user data?

5. What if any performance or cost considerations affect the use of encryption in the design of Tencent products?

6. Why was QQ Browser designed to transmit certain sensitive user data, such as all URLs visited by users, in an unencrypted format? Will Tencent correct this practice, and if so, when?

At Trinity College
1 Devonshire Place, Toronto, ON
Canada M5S 3K7
T: 416-946-8900 F: 416-946-8915

At the Observatory
315 Bloor Street West, Toronto, ON
Canada M5S 0A3
T: 416-946-8929 F: 416-946-8877

www.munkschool.utoronto.ca

7. Why does Tencent provide its QQ Browser software for download via HTTP rather than the more secure HTTPS?

8. The Windows version of QQ Browser contains a WUP request with the name qbindexblacklist.testUrl. Does this process compare a requested URL to a "blacklist" of websites? If so, what are the origins of the blacklist utilized in QQ Browser? Does this process require that a transmission be unencrypted in order to function properly?

9. Why does the Windows version of QQ Browser collect and transmit data regarding the version of Internet Explorer installed on the user's computer? What purpose does this data serve?

10. Why does the Windows version of QQ Browser encrypt data with a non-standard, modified TEA cipher using a non-standard modification of CBC as block cipher mode? Did Tencent design this encryption process? If not, what are its origins?

11. Was Tencent aware of the use by Baidu Browser of the same non-standard encryption implementation as mentioned in question 10 above? Did Tencent communicate with Baidu about this implementation?

12. Please provide a current timetable reflecting actual or estimated dates of completion of fixes for each of the vulnerabilities we reported to Tencent.

We plan to publish a report reflecting our research on March 28, 2016. We would appreciate a response to this letter from your company as soon as possible, which we commit to publish in full alongside our research report. Thank you.

Sincerely,

Professor Ronald J. Deibert
Director of the Citizen Lab
Munk School of Global Affairs
University of Toronto

At Trinity College
1 Devonshire Place, Toronto, ON
Canada M5S 3K7
T: 416-946-8900 F: 416-946-8915

At the Observatory
315 Bloor Street West, Toronto, ON
Canada M5S 0A3
T: 416-946-8929 F: 416-946-8877

www.munkschool.utoronto.ca