Responses Received from Baidu on February 22nd, 2016

1) Baidu Browser (Android version 6.2.18.0 and Windows version 7.6.100.2089) collects detailed and extensive user data, as documented in our correspondence. For example, the Windows version of Baidu Browser collects and transmits -- unencrypted -- the URL and title of all websites visited by a user, as well as the user's hard drive serial number and MAC address. Why is this sensitive user data collected in the first instance? Why is it transmitted insecurely?

Baidu endeavors to collect data in a way consistent with the highest standards of security and user privacy in the industry. We disclose our practices in our terms of service under privacy rights as detailed here (Chinese): https://www.baidu.com/duty/yinsiquan.html

We're grateful of Citizen Lab for being mindful of data security in transmission and we have already made substantial progress toward ensuring that any such transmission will be secure. Our timetable for making remaining changes to encrypted transmission are detailed below.

2) Which laws, regulations, or policies (internal or external) govern Baidu's collection of user data? What user data is Baidu required to collect pursuant to such law, regulation, or policy?

Unable to comment.

3) Does Baidu intend to alter its collection through its browser of certain types and amounts of user data? If so, what changes will be made, and when?

We will significantly strengthen information security, and complete changes to the mobile browser before the end of February and to the PC browser by early May of this year (2016).

4) For how long does Baidu retain the user data that it collects through its browser? How is that data stored, and what security measures are in place to protect that data at rest? Does Baidu share that data with third parties? and if so, with whom?

The time we retain data varies according to data type.

Data is stored in Baidu's Internet Data Centers, which are equipped with state-of-the-art security.

Pursuant to applicable laws, regulations and policies as well as Baidu's own stated terms of service, we guarantee protection of user data. While Baidu will sometimes share certain non-sensitive user data with commercial parties pursuant to applicable laws, regulations and policies, and will do so based on the nature of the relationship the company has with those parties, we will strictly protect all personal data, and will not share certain sensitive personal data with any third parties.

5) What if any laws, regulations, or policies (internal or external) guide Baidu's approach to the use of encryption in transmitting or storing user data?

Baidu’s own internal guidelines, while strict, can always be improved, and we welcome the input of other organizations in helping us to adhere to higher standards of encryption and storage. Individual regulatory agencies, for example the China Banking Regulatory Commission and the China Insurance Regulatory Commission, have strict guidelines for storage of user data. Our interest in working to better protect user data is about providing users with greater security—not only for compliance with any existing regulation.

6) Why was Baidu Browser designed to transmit certain sensitive user data, such as GPS coordinates and browser search queries, in an unencrypted format?

We have already switched over to encrypted formats for transmission of such data.

7) Why was Baidu Browser designed to use symmetric encryption and hard-coded keys, rather than asymmetric encryption?

The PC browser is in process of switching over to asymmetric encryption. The prevalence of older PCs that weren’t optimized for asymmetric encryption meant that our switch-over was somewhat delayed and will be completed by May. Progress has been much faster for mobile browser, and the switch-over to asymmetric encryption will be completed before the end of February.

8) What entities -- within or outside Baidu -- were involved in creation of the analytics software development kit (SDK) used in Baidu Android apps? Does Baidu subject its SDKs to any form of security audit or testing? Please describe that process.

Development of the analytics SDK was done internally. In light of recent experiences, we have greatly enhanced the auditing process of the SDK used in Android apps, and the SDK is subject to routine security auditing. We use our SDL (Security Development Lifecycle), built to the same standards as leading global software developers in all of our product development and auditing.

9) Why does the Windows version of Baidu Browser contain a feature to automatically proxy requests to certain websites hosted outside of China? Is this feature related to the partnership between Baidu and CloudFlare announced in September 2015?

[First question:] Unable to comment.

No, this had nothing to do with the CloudFlare partnership.

10) Did Baidu seek the approval of the Chinese government in order to enable the aforementioned proxy request feature of the browser? Is Baidu required by authorities to collect any user data as a condition to providing uncensored web access through its proxy feature? What data related to the proxy feature is Baidu required to share with the Chinese government?

Unable to comment.

11) Why do the Baidu proxy servers allow access to domains that are additional to those for which the browser uses the proxy? Does this disparity serve a particular technical or other function?

This was in response to popularity of *haitao*, or overseas e-commerce shopping, to speed load times of sites that tended to load slowly.

12) Please provide a current timetable reflecting actual or estimated dates of completion of fixes for each of the vulnerabilities we reported to you. Additionally, how does Baidu intend to address the use by third-party apps of vulnerable versions of its SDK?

By end of February, the Android browser will be fully encrypted and will use asymmetric encryption; by early May, the PC version will be fully encrypted.

We've improved the security review process and notified third-party app developers using previously vulnerable versions of certain SDKs, and we will continue to increase our security review and auditing process to ensure that the SDKs used by third parties are safe.