1. Does the U.S. Intelligence Community (IC) assess that mobile applications developed, operated, or owned by foreign entities are a potential national security risk?

Mobile applications developed, operated or owned by foreign entities present a potential national security risk because developers can deliberately code *kill switches*, *backdoors* or vulnerable data streams into mobile applications that allow access to the application's software, application-generated data, or even—in some cases—the device itself, and because application owners/operators can filter, censor, corrupt, intercept, and illegitimately divert or share data generated by applications.

- The mobile applications development industry is both global and highly collaborative, and applications developed by foreign entities may not be clearly distinguishable from those developed domestically. A large percentage of U.S. companies probably operate and serve customers using at least some mobile applications developed overseas in whole or in part.

Although there is additional risk associated with the broad use of mobile applications owned or operated by foreign countries, or that store data in those countries, foreign governments—through cooperative commercial enablers or front companies—can trivially gain access to large quantities of very granular U.S. person data through other means, to include buying data.

Generally, the key risk factors from foreign-developed applications are:

- Clear foreign government intent to harm U.S. interests;
- Technical skills and capabilities that would enable them to conduct supply chain operations;
- The nature of the information produced, collected, or stored by an application. For example, an application that stores and/or accesses users' sensitive communications or personal information may incur higher risks than an application that stores only the user's progress in a game;
- A legal/governance regime that would enable the foreign country to easily utilize commercial application developers for their foreign intelligence operations. As an example, China's National Security Law, Counterterrorism Law, Cybersecurity Law, and other laws and regulations codify the Chinese Government's ability to compel Chinese companies to cooperate with Chinese security services.

2. Does the IC assess that mobile applications that store or house information about U.S. citizens overseas are a potential national security risk?

Mobile applications that store or house information about U.S. citizens overseas vary in the potential magnitude of their national security risk—relative to mobile applications that store information in the United States—depending on several factors:

- Intent (and capacity) of the data-hosting government to harm U.S. interests;

- Legal/governance regime of the data-hosting country; the highest risk is in cases where the host government is able to compel its domestic commercial firms to cooperate with its security services to share commercial data those firms have collected from U.S. customers;

- Data privacy/protection/encryption regulatory regime of the data-hosting government;

- Data protection/encryption/IT security practices of managers of data stores (hosting providers, etc.) utilized by the application owners/operators.

3. Are there particular countries that the IC and the FBI assess to be exploiting or leveraging mobile applications to collect information on U.S. citizens?

To the extent that foreign-developed or -owned mobile applications from countries that pose an intelligence threat gain wide use in the United States, these foreign governments likely would exploit U.S. users' data in at least some cases. As an example, applications developed by Chinese companies—typical of mobile applications wherever developed—regularly transmit various categories of data about the mobile user (e.g., location data) to their parent companies. Such sharing of commercial data with the state is much more likely in authoritarian and illiberal states than in nations with an independent private sector and robust rule of law that legally enshrine civil liberties and privacy protections.

- In 2019, malware was pre-installed on Chinese manufactured mobile phones that were given to U.S. citizens as part of an American assistance program.

- In 2019, Chinese company Meiya Pico, one of China's largest computer forensics companies, produced a mobile application called MFSocket that allows Chinese law enforcement to spy on its citizens. The software, which was being installed by Chinese police during random street checks even when they are not suspected of a crime, provides access to images, audio files, location data, call logs, messages and the phone's calendar and contacts, including those used in the secure messaging application *Telegram*.

- In 2019, China's border authorities routinely installed a policing application called "Fengcai" on smartphones of travelers—including foreigners—who enter Xinjiang by land from Central Asia. The application gathers personal data from phones, including text messages and contacts, and checks for the presence on the devices of tens of thousands of specific files, and sends a report to a computer server. Artifacts in the source code suggest that the application was made by a unit of Nanjing FiberHome StarrySkay Communication Development Company, a unit of FiberHome, a producer of optical cable and telecom equipment that is partly owned by the Chinese state that offers products—including cellphone forensic equipment—to help police collect and analyze data.

As another example, Russian firms that develop, own or operate mobile applications would be unable to resist attempts by Moscow to compel them to share U.S. person data that they collect.

4. Are there particular mobile applications, developers, or companies that the IC and the FBI assess to be willfully sharing information on U.S. citizens with foreign governments?

We note that industry has at times identified mobile malware created by cyber criminals probably to steal banking information for financial gain, and that app stores periodically remove suspicious applications from their inventories.

5. Are there particular mobile applications, developers, or companies that the IC and the FBI assess to be especially vulnerable to undue foreign government influence?

Countries that pose an intelligence threat to U.S. interests are more likely to pressure companies to bow to its influence compared against lower threat nations. As such, vulnerability will be potentially expansive as it will apply to several companies with business interests across multiple nations and can be based on such factors as market share, opportunity, and risk calculus by foreign governments.

- This year, the Chinese government compelled *Zoom* – a U.S. company with research and development offices in China – to block the virtual activities of political activists living outside of China. In 2019, former U.S.-based employees at *TikTok* alleged that moderators in China directed them to censor problematic videos deemed subversive or controversial to the Chinese government. Employees of *TikTok* in the United States were pressured to censor 'culturally problematic' content that might offend the Chinese government.

- As of early 2019, Chinese authorities were obtaining personal data from the phones of tourists entering China's far western region of Xinjiang using a secretly installed mobile app.

- In early 2018, before *Tencent* began contributing data to the national identity database, Beijing temporarily stopped approving the company's new video games, causing *Tencent* to experience its first profit drop in 13 years.

- *ToTok*—an Emirati mobile messaging application that was downloaded millions of times, including by users in North America—is sponsored by the Emirati government. It collects user location and contacts, and has access to users' microphones, cameras, calendar and other phone data.

- The Russian firm Kaspersky—which markets a mobile application—is an especially lucrative target for undue foreign government influence because of its wide market share.