

Appendix I: Letters to CETC, HBFEC, Chen Quanguo, and Wang Mingshan

February 11, 2019

Mr. Xiong Qunli
Chairman
China Electronics Technology Group
27 Wanshou Road, Haidan District
Beijing, 100846
China

Mr. Wang Tienmeng
Chairman
Hebei Far East Communication System Engineering Co., Ltd.
21 Changsheng Street, Luquan Economic Development Zone
Shijiazhuang, 050200
China



Re: Collection and use of personal data in Xinjiang

Dear Chairman Xiong and Chairman Wang,

Human Rights Watch is an independent nongovernmental organization that monitors and reports on compliance with international human rights standards in more than 90 countries around the world. We have been reporting on and advocating solutions to human rights abuses in China for over 20 years.

We are currently researching the collection and use of personal information by the Xinjiang Public Security Bureau. The research is intended to show whether and how Chinese authorities have complied with domestic law and fulfilled their obligations to protect privacy rights under international human rights law.

Human Rights Watch understands that China Electronics Technology Group Corporation (CETC 中国电子科技集团公司) has supplied a policing and big data platform called the Integrated Joint Operations Platform (IJOP) to the Xinjiang Public Security Bureau.

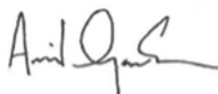
We also understand that Hebei Far East Communication System Engineering Company (HBFEC, 河北远东通信系统工程有限公司), a company partly owned by CETC, has developed a mobile app for police officers and government officials to send information to and receive information from the central IJOP system.

In the interest of thorough and accurate reporting, we are writing to request further information and other perspectives you may have about your activities in this regard. We would appreciate your response to the following questions:

1. Can you confirm that CETC and HBFEC are designated suppliers of the IJOP system and app used by the Xinjiang Public Security Bureau? If so, can you provide further details about those contracts with the government?
2. Based on our examination of the IJOP system, we understand that the app prompts police officers and government officials to collect a wide range of personal information from people in Xinjiang. Can you confirm that this is the case, and, if so, can you:
 - a. Provide details on what kinds of information government officials are collecting through the IJOP app?
 - b. Explain who is subject to such information collection?
 - c. Describe the intended use of such information?
3. We understand that the IJOP app is also used to identify certain “problematic” individuals, vehicles, or events, and sends officials to investigate and provide feedback.
 - a. Can you confirm that this is the case? If so, can you provide details about these tasks or investigations?
 - b. Can you provide details about precisely how the IJOP system conducts its analysis, and how it identifies “problematic” people?
4. One government WeChat article acknowledged that the IJOP system is contributing data and analysis that have been used to identify targets to be detained in “political education” centers in the ongoing “Strike Hard Campaign against Violent Extremism.” Can you explain how IJOP systems’ analytics contribute to the detention of people in these facilities?
5. Do you review past sales to ensure your products and services are not used inappropriately, such as by violating international or domestic human rights standards, including privacy? If so, what steps do you take if issues are identified?
6. Do you have any policies and procedures in place to evaluate the design, production, marketing, or use of your products in light of human rights standards? If so, can you provide us details?
7. Did your company conduct any due diligence to determine whether there might be any adverse human rights impact from its use by authorities in Xinjiang?

To be able to reflect your response in our forthcoming publication, we would welcome a response to these questions and any other comments you may have by March 4, 2019. Thank you for your assistance in these matters.

Sincerely,



Arvind Ganesan
Director, Business and Human Rights Division
Human Rights Watch



Sophie Richardson
China Director
Human Rights Watch

March 21, 2019

Chen Quanguo
Party Secretary of the Xinjiang Uyghur Autonomous Region
Chinese Communist Party Xinjiang Uyghur Autonomous Region
2 Jiankang Road, Tianshan Qu, Urumuqi 830003, Xinjiang



HRW.org

Re: Collection and Use of Personal Data in Xinjiang

Dear Party Secretary Chen,

Human Rights Watch is an independent nongovernmental organization that monitors and reports on compliance with international human rights standards in more than 90 countries around the world. We have been reporting on and advocating solutions to human rights abuses in China for over 20 years.

We are currently researching the collection and use of personal information by the Xinjiang Public Security Bureau. The research is intended to show whether and how Chinese authorities have complied with domestic law and fulfilled their obligations to protect privacy rights under international human rights law.

Human Rights Watch understands that the China Electronics Technology Group Corporation (CETC 中国电子科技集团公司) has supplied a policing and big data platform called the Integrated Joint Operations Platform (IJOP) to the Xinjiang Public Security Bureau.

We also understand that Hebei Far East Communication System Engineering Company (HBFEC, 河北远东通信系统工程有限公司), a company partly owned by CETC, has developed a mobile app for police officers and government officials to send information to and receive information from the central IJOP system.


In the interest of thorough and accurate reporting, we are writing to request further information and other perspectives you may have about your activities in this regard. We would appreciate your response to the following questions.

1. Can you confirm that CETC and HBFEC are designated suppliers of the IJOP system and app used by the Xinjiang Public Security Bureau? If so, can you provide further details about those contracts with the two companies?
2. Based on our examination of the IJOP system, we understand that the app prompts police officers and government officials to collect a wide range of personal information from people in Xinjiang. Can you confirm that this is the case, and, if so, can you:
 - a. Provide details on what kinds of information government officials are collecting through the IJOP app?
 - b. Explain who is subject to such information collection?
 - c. Describe the intended use of such information?
3. We understand that the IJOP app is also used to identify certain “problematic” individuals, vehicles, or events, and send officials to investigate and provide feedback.
 - a. Can you confirm that this is the case? If so, can you provide details about these tasks or investigations?

- b. Can you provide details about precisely how the IJOP system conducts its analysis, and how it identifies “problematic” people?
4. One government WeChat article acknowledged that the IJOP system is contributing data and analysis that have been used to identify targets to be detained in “political education” centers in the ongoing “Strike Hard Campaign against Violent Extremism.” Can you explain how IJOP systems’ analytics contribute to the detention of people in these facilities?

To be able to reflect your response in our forthcoming publication, we would welcome a response to these questions and any other comments you may have by April 3, 2019. Thank you for your assistance in these matters.

Sincerely,



Sophie Richardson
China Director
Human Rights Watch

Cc:
Wang Mingshan, Chief of Police Security Department of Xinjiang Uyghur Autonomous Region

Appendix II: Screens Related to Supervision of Officials



Fig.28: A screenshot entitled “leader supervision” showing how supervisors can keep tabs on lower-level officials as they accomplish IJOP-related tasks.



Fig.29: A screenshot entitled “my score” evaluates officials’ progress accomplishing IJOP-related tasks.

Appendix III: Screens Related to Search Function



The screenshot shows a mobile application interface for searching information. At the top, there is a status bar with icons for signal, Wi-Fi, and battery, and the text "98% 12:00". Below this is a dark blue header with a back arrow on the left, the title "信息搜索" (Information Search) in the center, and a "搜索" (Search) button on the right. The main content area consists of five input fields, each with a label on the left and a placeholder on the right:

所在地区	请选择
姓名	请输入
身份证号	请输入
建筑地址	请输入
户号	请输入

Below the input fields is a light blue section labeled "搜索结果" (Search Results), which is currently empty.

Fig.30: Screenshot showing how officials can search for information about people.

96% 11:53

全息档案权限申请

被核查人身份证号 请输入被核查人员身份证号

申请人姓名 请输入

申请人警号 请输入

申请人手机号码 请输入

申请人单位 请输入

申请原因 请输入

审批人姓名 未选择

申请时效 30天 (申请通过后, 30天内有效)

提交申请

Fig.31: Screenshot showing how officials can access the “full profile” of a given individual.

Appendix IV: Screens Related to Filing Reports



Fig.32: Screenshot showing how officials can search for incident reports filed concerning suspicious vehicles, objects, people, or about internal migrants.



Fig.33: This is how officials can log an incident report.



Fig.34: Screenshot showing details of an incident report.



Fig.35: This is how officials can log a report about a person they find problematic.



Fig.36: This is how officials can log an object they find problematic.