To:

Ursula von der Leyen
President of the European Commission

Thierry Breton
Vice-President of the European Commission

18 October 2021
Brussels, Belgium

Regarding Security Risks of Xiaomi and Huawei Smartphones

We, the undersigned Members of the European Parliament, would like to express our concerns related to the use of Chinese mobile communication technology and urge the Commission to take appropriate action to safeguard the privacy of mobile users and the freedom of the information space in Europe.

On September 21, Lithuania's National Cyber Security Centre (NCSC) published a report[1] highlighting security, privacy and free speech concerns associated with the use of smartphones produced by Chinese manufacturers Xiaomi and Huawei. A technical assessment of recent 5G enabled models has revealed features that collect and transfer excessive personal information, expose users to cybersecurity risks and malware, and automatically censor downloaded content if it is not in line with Beijing's policy at home and abroad. The findings complement the data of the international Common Vulnerabilities and Exposures database that identifies dozens of vulnerabilities across older generation Xiaomi and Huawei devices. In response to the study, Lithuania's Ministry of National Defence called for caution when using Xiaomi and Huawei smartphones analysed in the report.

Lithuania's NCSC report relates to a broader problem of risks posed by smartphones and telecommunication technology produced by China's manufacturers. EU and its member states have already largely acknowledged the cybersecurity and privacy risks associated with China's investment in critical infrastructure across the EU and in the rollout of 5G technology in particular. Commission's 2019 risk assessment report for cybersecurity in 5G networks warns against suppliers that have close links to the governments of undemocratic states, while the US, Australia and a number of individual EU member states have explicitly or implicitly banned China's 5G manufacturer Huawei from investing in their 5G infrastructure.

In addition to a growing consensus over the need to limit China's investment in critical infrastructure, there are increasing concerns over cyber espionage in Europe. Most recently, we discovered the information about ongoing series of cyberattacks in France performed by APT31 group, closely associated with the government of China. In July 2021, the French

[1] The report consists of the initial 23 August Report and 27 September Amendment.

cybersecurity agency ANSSI announced that ATP31 had used a large network of Wi-Fi routers across France to conduct "stealth reconnaissance as well as attacks". The High Representative Joseph Borrell has addressed this in his July 19 statement urging the Chinese authorities to adhere to the norms of responsible state behaviour and "not allow its territory to be used for malicious cyber activities."

Finally, China's disinformation, academic censorship, and political interference through social networks and media organizations are growing sources of concern across Europe and in its immediate neighbourhood. Last year, the Commission named China as one of the main sources of COVID-19 related disinformation in its communication on 'Tackling COVID-19 disinformation". European Parliament, in its 16 September 2021 resolution on EU-China strategy, expressed its concern about disinformation campaigns stemming from China and highlighted the need to "equip the EEAS with a mandate and the necessary resources to monitor and address Chinese disinformation operations, including the creation of a dedicated Far-East StratCom Task Force focused on disinformation emanating from China."

The recent Lithuania's National Cyber Security Centre report relates to all of the concerns already widely expressed by the EU and its member states about cybersecurity of critical telecommunications infrastructure, cyber espionage and protection of private data, and disinformation and growing reach of China's censorship.

In light of this, we urge the Commission to step up the cooperation at the EU level and to set common standards and approach for the use of unreliable information and communication technologies that take into account technological risks and national security considerations associated with their use. We would like to inquire, what specific steps the Commission will take to address the concerns highlighted in this letter.

Sincerely,

Members of the European Parliament

Rasa JUKNEVIČIENĖ (EPP, Lithuania)
Ioan-Dragos TUDORACHE (Renew, Romania)
Aušra MALDEIKIENĖ (EPP, Lithuania)
Radan KANEV (EPP, Bulgaria)
Yannick JADOT (Greens / EFA Group, France)
Ivan ŠTEFANEC (EPP, Slovakia)
Gianna GANCIA (ID, Italy)
Hermann TERTSCH (ECR, Spain)
Reinhard BÜTIKOFER (Greens / EFA Group, Germany)
Miriam LEXMANN (EPP, Slovakia)
Inese VAIDERE (EPP, Latvia)
Dace MELBARDE (ECR, Latvia)
Isabella ADINOLFI (EPP, Italy)
Vladimír BILČÍK (EPP, Slovakia)
Raphaël GLUCKSMANN (S&D, France)
Rosa D'AMATO (Greens / EFA Group, Italy)
Andrius KUBILIUS (EPP, Lithuania)
Francois ALFONSI (Greens / EFA Group, France)
Benoit BITEAU (Greens / EFA Group, France)
Damien CAREME (Greens / EFA Group, France)
David CORMAND (Greens / EFA Group, France)

Gwendoline DELBOS-CORFIELD (Greens / EFA Group, France)
Karima DELLI (Greens / EFA Group, France)
Claude GRUFFAT (Greens / EFA Group, France)
Michèle RIVASI (Greens / EFA Group, France)
Caroline ROOSE (Greens / EFA Group, France)
Mounir SATOURI (Greens / EFA Group, France)
Marie TOUSSAINT (Greens / EFA Group, France)
Salima YENBOU (Greens / EFA Group, France)
Juozas OLEKAS (S&D, Lithuania)
Eva KAILI (S&D, Greece)
François-Xavier BELLAMY (EPP, France)