Home Office

Home Secretary
2 Marsham Street
London SW1P 4DF
www.gov.uk/home-office

Mr Arnie Stepanovich
Access Now
arnie@accessnow.org

21 September 2017

Dear Arnie,

Thank you for your letter of 30 June in relation to encryption. I would like to reassure you that the British Government strongly supports a free, open and secure internet and we continue to make significant international commitments to protect and defend citizens' freedom to express themselves online and their right to privacy. In 2012 the UK co-sponsored the 2012 UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the internet, and just this year we adopted the Brazilian and German-sponsored 2017 Human Rights Council resolution on the right to privacy in the digital age '*emphasising that in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association.*'

I strongly believe that encryption plays a fundamental role in protecting UK citizens online and is key to growing the digital economy and delivering public services. We are committed to making the UK the safest and best place to do business online. That is why we have established the world class National Cyber Security Centre to provide expert advice and guidance to the public and private sector, including the use of strong encryption, as well as to lead our response to cyber incidents.

However, like many powerful technologies, encrypted services are abused by a small minority of people. Communications providers should not want terrorists to be able to plot mass murder on their platforms in secret or for serious criminals to use their services to facilitate the importation of drugs or the trafficking of vulnerable people, safe from police action. But if our law enforcement or security and intelligence agencies cannot see what a terrorist or criminal is planning then they cannot stop them. The fact that our agencies are unable to access end-to-end encrypted messages sent by terrorists and serious criminals – even with a warrant signed off by a Secretary of State and, under the Investigatory Powers Act, a senior judge – is a real problem for investigations today. Whether or not a terrorist or criminal can be lawfully investigated should depend on the threat they pose or the crime they are planning, not on what app they have downloaded.

That is why the UK Government along with our counterparts in the Australian, Canadian, New Zealand and American Governments, and leaders of the G20 and EU Member States, including France and Germany have all come to the same conclusion: the inability to gain access to end-to-end encrypted data in an intelligible form in specific and targeted instances is severely impacting our agencies' ability to stop terrorist attacks and bring criminals to justice.

The UK Government does not want unfettered access to all communications, and we do not want to be able to decrypt and read everyone's communications all of the time. We do not want technology companies to create a universal key or a so-called backdoor into their systems. And we have no intention of banning end-to-end encryption or of trying to weaken the security of industry standard encryption that is used to secure the global trade and communications we rely upon in our daily lives. But we do intend to work with the technology companies to better understand the decisions they have made whilst implementing encryption within their services and identify ways for our law enforcement and intelligence services to gain specific information about what serious criminals and terrorists are doing online, without compromising wider safety and security of their systems for lawful users.

The responsibility for tackling this threat at every level lies with both governments and with industry and it is absolutely crucial that companies acknowledge the vital role they have to play. So we are working closely with them to find a solution to protect our citizens from terrorists and criminals who might abuse their services. This is not about compromising wider security. It is about working together so we can find a way for our law enforcement and intelligence services, in very specific circumstances, to get more information on what serious criminals and terrorists are doing online. I am sure you will share our view that encryption should not be a vehicle for crime and terrorism.

You may have seen that recently the major communications service providers launched a Global Internet Forum to Counter Terrorism (GIFCT). This industry-wide and global forum will focus on developing innovative technical solutions; supporting smaller companies – sharing knowledge and best practice; and research and analysis to improve their response to tackling terrorist use of the internet. I urge you to participate in the Forum and aid industry in making it a success.

The Rt Hon Amber Rudd MP