New American

Written by **Luis Miguel** on November 11, 2020

Big Brother: EU Wants to Create Backdoor in Encrypted Messaging Apps

How dare the people try to keep their conversations private from Big Brother?

Delmaine Donson/iStock/Getty Images Plus

The European Union Council's internal documents show that the bloc now wants to ban end-to-end encryption on messaging services such as WhatsApp and Signal in response to recent Islamic terror attacks in France and Austria.

A draft resolution from the European Resolution on encryption, dated November 6, said that while the EU considers encryption a useful tool for protecting citizens' privacy, it has been a roadblock to law enforcement's efforts to combat terrorism, organized crime, child exploitation, and cybercrimes.

Thus, the resolution called for the EU to mandate that messaging services using end-to-end encryption also create a backdoor so that government can access private messages, putting an end to any semblance of privacy the apps may have offered.

The document reads:

> For competent authorities, access to electronic evidence is not only essential to conduct successful investigations and thereby bring criminals to justice, but also to protect victims and help ensure security.
>
> Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organised crimes and terrorism, including in the digital world, are extremely important. Any actions taken have to balance these interests carefully.

The Austrian broadcaster ORF pointed to last month's Islamic terror attack in Vienna as an impetus for the change. But as the outlet notes, the Austrian counterterrorism agency BVT has received a warning from Slovakian intelligence about the threat posed by the terrorist, and therefore having a backdoor into the messaging services would not have made a difference.

Ray Walsh of ProPrivacy told the tech website IT Pro that "a European Union move to ban encryption from messaging platforms like WhatsApp and Signal would be a massive threat to data privacy as we know it. It is a disappointing change in approach from the EU which has previously been pro-privacy for European citizens."

"Security experts understand that the EU government's contention that 'strong encryption technology' can coexist with purposefully designed backdoors is contrary to the principles of robust cryptography," Walsh said, going on to warn, "Not only is breaking encryption a threat to national security, but the ability to communicate privately is a vital part of any free society."

The resolution will be presented to the Council of Permanent Representatives of the EU Member States (COREPER), where it can pass without any debate.

Lord Daniel Moylan of Britain, reacting to the EU's attempted assault on encrypted messages, said: "Thank God we got out. It would have been excruciating hearing Remainers defend this."

Moreover, the British anti-government surveillance campaign group Big Brother Watch warned: "Make no mistake: they are trying to ban the right to a private conversation."

Curiously, the European Union is now concerned about dealing with Islamic terror; but their solution is to violate the fundamental rights of their law-abiding citizens instead of doing the obvious: Enacting a rational migration policy that doesn't flood European countries with hostile migrants from the Middle East.

Migration in large numbers will nearly always lead to civil strife due to clashes of culture and religion, especially when you have a religion, such as Islam, that treats individuals of other faiths as "infidels" seen with contempt. This is simply the nature of humans and societies, and anyone who has taken even a cursory glance at a world history book would tell you that unchecked migration of the type that the EU has been forcing upon its member countries is a bad idea.

The globalist elites who back both the migration and anti-encryption policies, however, *do* understand history. They are acting deliberately as they always do to achieve their desired ends of bigger, more invasive government with less freedom.

First, they create a problem with a bad policy such as mass migration. Then, when their actions bring devastating results such as terrorism, they don't resolve it with the obvious solution of rescinding their original bad policy (which would mean stopping mass migration), but instead institute stricter government controls (such as banning end-to-end encrypted messages), paving the way to totalitarianism one step at a time.