UK and US sign landmark Data Access Agreement

The world-first UK-US Bilateral Data Access Agreement will dramatically speed up investigations and prosecutions by enabling law enforcement, with appropriate authorisation, to go directly to the tech companies to access data, rather than through governments, which can take years.

The Agreement was signed with US Attorney General William P. Barr in Washington DC, where the Home Secretary also met security partners to discuss the two countries' ever deeper cooperation and global leadership on security.

Home Secretary Priti Patel said:

> Terrorists and paedophiles continue to exploit the internet to spread their messages of hate, plan attacks on our citizens and target the most vulnerable.
>
> As Home Secretary I am determined to do everything in my power to stop them. This historic Agreement will dramatically speed up investigations, allowing our law enforcement agencies to protect the public.
>
> This is just one example of the enduring security partnership we have with the US and I look forward to continuing to work with them and global partners to tackle these heinous crimes.

US Attorney General William P. Barr said:

> This Agreement will enhance the ability of the United States and the United Kingdom to fight serious crime – including terrorism, transnational organized crime, and child exploitation – by allowing more efficient and effective access to data needed for quick-moving investigations.
>
> Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats.
>
> This Agreement will make the citizens of both countries safer, while at the same time assuring robust protections for privacy and civil liberties.

The current process, which see requests for communications data from law enforcement agencies submitted and approved by central governments via Mutual

Legal Assistance (MLA), can often take anywhere from six months to two years. Once in place, the Agreement will see the process reduced to a matter of weeks or even days.

The Agreement will each year accelerate dozens of complex investigations into suspected terrorists and paedophiles, such as Matthew Falder who was sentenced in 2018 of 137 offences after an eight-year campaign of online child sexual abuse, blackmail, forced labour and sharing of indecent images. His case highlights the need to speed up these investigations.

The US will have reciprocal access, under a US court order, to data from UK communication service providers. The UK has obtained assurances which are in line with the Government's continued opposition to the death penalty in all circumstances.

Any request for data must be made under an authorisation in accordance with the legislation of the country making the request and will be subject to independent oversight or review by a court, judge, magistrate or other independent authority.

The Agreement does not change anything about the way companies can use encryption and does not stop companies from encrypting data.

It gives effect to the Crime (Overseas Production Orders) Act 2019, which received Royal Assent in February this year and was facilitated by the CLOUD Act in America, passed last year.

Open letter to Facebook Chief Executive Mark Zuckerberg

The Home Secretary has also published an open letter to Facebook, co-signed with US Attorney General William P. Barr, Acting US Homeland Security Secretary Kevin McAleenan and Australia's Minister for Home Affairs Peter Dutton, outlining serious concerns with the company's plans to implement end-to-end encryption across its messaging services.

Addressed to Facebook's CEO, Mark Zuckerberg, the letter calls for a halt to the proposals unless the company can provide assurances that there will be no reduction in Facebook's ability to keep its users safe and enable law enforcement access to content in exceptional circumstances in order to protect the public.

This issue is not just about one company. However, the letter makes clear particular concerns with Facebook's plans and the impact they would have on efforts to tackle online child sexual abuse and terrorism.

Facebook's proposals would put its own vital work keeping people safe at risk. In 2018, Facebook made 16.8 million reports of child sexual exploitation and abuse content to the US National Center for Missing & Exploited Children (NCMEC), 12 million of which it is estimated would be lost if the company pursues its plan to implement end-to-end encryption. The National Crime Agency estimates that these referrals from Facebook have led to more than 2,500 arrests in 2018 and almost 3,000 children safeguarded.

The Government is clear in its commitment to the right to privacy and does not, however, believe the requirement to provide exceptional access to data where a warrant is in place, undermines this in any way. Law enforcement and other agencies must, in certain circumstances, be able to access data, with strong and independent authorisation and oversight.

The Home Secretary added:

> Tech companies like Facebook have a responsibility to balance privacy with the safety of the public.
>
> So far nothing we have seen from Facebook reassures me that their plans for end-to-end encryption will not act as barrier to the identification and pursuit of criminals operating on their platforms.
>
> Companies cannot operate with impunity where lives and the safety of our children is at stake, and if Mr Zuckerberg really has a credible plan to protect Facebook’s more than two billion users it’s time he let us know what it is.