Written Testimony of

Mr Paddy McGuinness
United Kingdom Deputy National Security Adviser

Before the

Judiciary Sub-Committee on Crime and Terrorism
United States Senate

May 10, 2017

Overview

The United States and the United Kingdom have a shared history, values and a unique relationship that has benefited our countries. Our Governments' highest priority is to protect our people.

We face unprecedented threats from serious crime, including terrorism. Trans-national crimes, such as child sexual exploitation, human trafficking and drug smuggling necessarily span different jurisdictions and affect citizens globally. Terrorists coordinate, inspire and direct threats across borders, and exploit the activities of serious criminals.

The way people communicate has changed. Internet-based communications technologies are now used by most of us every day. Criminals, and especially terrorists, use these services. Limited and proportionate access to the content of their communications is vital to keep our citizens and allies safe.

Most communications services are operated by companies based in the United States. These companies tell us that US law prevents them disclosing content to the UK, in most circumstances, even where required to, under our law.

Our Governments have been working with US technology companies on a proposed UK-US Bilateral Agreement on Data Access. This would be about reciprocal targeted access to data, enabling companies based in one country to comply with lawful orders from the other. US nationals and persons in the US would be excluded. Such an Agreement would recognise the high standards of authorisation and oversight that the UK and US have in place.

The UK's Parliament passed legislation in 2016 that strengthened its already robust investigatory powers framework by introducing judicial authorisation, and making such international agreements possible in UK law. However, for the UK and US Governments to progress and sign a Bilateral Agreement, legislative change is required in the US to make provision for such Agreements.

Her Majesty's Government is committed to resolving this issue in a way that preserves an open internet and protects privacy and freedom of speech.

The Problem

The content of communications between two people in the UK, planning or committing a serious crime, such as a terrorist act, can be beyond the reach of the UK law enforcement and security agencies. US technology companies have been most successful in developing and marketing their services. They have a preponderant share of the market in the UK. In many cases, companies say that US law prevents them from cooperating with lawful UK orders and this limits profoundly the UK's ability to access data that can be critical for disrupting or preventing threats to our citizens.

US companies can comply with requests for communications metadata: that is the "who, where, when and how" of the communication. But it is often the "what", for example the content of email and instant messages, which is the vital information that can help stop violence and bring a criminal to justice.

Perhaps the most egregious example of this is terrorist use of the internet to direct and inspire violent attacks in many countries with no respect for borders or jurisdictions. The UK has disrupted 13 attack plots since May 2013 and many more individuals or groups of individuals working involved in terrorist related activity. The 22 March attack at Westminster Bridge and our Parliament in which five people were killed, including a US citizen from Utah, is a reminder that attacks cannot be wholly prevented. It is noteworthy that there have been multiple arrests for terrorism offences since then – one also in the vicinity of the Westminster Parliament. Virtually all involved in terrorism make use of some communication service provided by US companies.

The importance of access to communications to disrupt terrorism was demonstrated most memorably in 2006, when terrorists in the UK and Pakistan plotted to detonate explosives on multiple transatlantic airlines en-route to the US. Their plot involved constructing liquid based improvised explosive devices in an effort to bypass airport security controls. If it had succeeded, the plot could have led to the deaths of hundreds of UK, American and other nationals.

The UK's ability to access the communications of the perpetrators was critical to the disruption of that plot and the prosecution of the terrorists. But since 2006, ever more communication is taking place via new messaging providers, the majority based in the United States.

The US technology companies have done what they can to assist. However, this falls short of what is required to detect and prevent terrorist plots. It leaves the companies in the invidious position of having to withhold information that could protect public safety. They want this resolved.

The increasing use of technology operating under current US law presents a stark problem for tackling other serious crime beyond terrorism, as well. US companies currently respond with data to only a very small proportion of the UK's requirement for the content of communications in these cases. This issue can mean that, for instance, a UK-led investigation into paedophiles, distributing images globally, cannot be progressed so that the paedophiles remain at large.

It does not make sense that two criminals plotting a major drug deal, a murder, a kidnap, trafficking people or sexually abusing a child in the UK can have their communications intercepted if they communicate via text message, but if they use a US company's services their data should be out of reach of UK law enforcement.

Lack of transparent frameworks for accessing data across borders incentivises governments to require companies to control data within their own national territories to ensure access for their law enforcement agencies ("data localisation"). This is not in companies', Governments' or citizens' interests: it increases the costs of doing business, reduces the efficiency of the services and potentially drives data into jurisdictions where the rule of law and protections around freedom of speech and human rights are considerably weaker.

The current legal situation is **bad for public safety, bad for companies and bad for privacy**.

Solution: Bilateral Data Access Agreement

To address this problem, our Governments have been working with the companies on a proposed UK-US Bilateral Agreement on cross-border access to data. The Agreement would recognise the high standards of authorisation and oversight that the UK and US have in place and allow companies based in one country to comply with lawful orders for the contents of electronic communications from the other. The Agreement is specifically intended to permit access to data to combat serious crimes, including terrorism.

It would include strong safeguards and maintain rigorous privacy protections for US persons. **The UK could only use the Agreement to request data on non-US persons located outside the US.**

For an Agreement to be possible, Congress would need to amend US law to remove the legal bar preventing US companies from complying with lawful UK requests for data.

The Benefits

The Agreement will show that governments can work constructively with industry and law makers to **overcome potential jurisdictional conflicts** and **improve public safety** with due regard for transparency, online freedoms and the rule of law. Major US technology companies are supportive as this Agreement protects them from conflicts of law and enables them to resist calls from countries with lower privacy standards to hand over data. It also reduces the risk of a US company unwittingly hosting communication which leads to a terrorist attack or major crime. Independent academics have written in support of such a framework. An Agreement would:

- Ensure access to the data across borders needed to **prevent serious crimes and threats from terrorism,** while **protecting privacy and freedom of speech.**
- Support **an open and efficient internet by reducing incentives for Governments to impose data localisation requirements**. These incentives

risk creating a "balkanised", or fragmented, internet. That would be bad for US and global business.

- **Prevent conflicts of laws** which can harm companies operating across borders; in complying with one country's laws, they may infringe another's.
- Provide **an incentive for other countries to improve their standards of privacy protection, oversight and authorisation** in order to be party to similar agreements in the future.
- **Reduce the burden on Mutual Legal Assistance Treaty (MLAT) mechanisms** and Government resources by ensuring that requests authorised in one country are transmitted directly to the relevant company.

Key Principles of an Agreement

The Department of Justice published a White Paper in March 2016 outlining the key principles for US legislation to resolve these issues, and any Bilateral Agreement. This was followed by a legislative proposal that was sent to Congress in July 2016. **Her Majesty's Government is in full agreement with the principles outlined in these documents.** In particular we agree that the agreement should:

i. **Not allow the UK to get data on US nationals or anyone in the US**.

ii. Limit access to **targeted** orders for data (i.e. a specific individual, phone number, email address or other identifier), and **not bulk** access to data.

iii. Be limited to **prevention, detection, investigation or prosecution of serious crime**, including terrorist activity or the proliferation of chemical, biological, radiological or nuclear weapons.

iv. Permit orders for **"surveillance"** or **"real-time"** access in order **to prevent** attacks and crimes before they occur.

v. Be **"encryption neutral"**. Any Agreement should not include terms on encryption which should continue to be discussed by Governments and companies as a separate issue.

Mutual Legal Assistance Treaties are important, but they are not the answer to the cross border data problem. They are designed for obtaining evidence **after** a crime has been committed. Even in those cases, it can sometimes take too long to receive the necessary evidence in order to progress an investigation and secure convictions. It is widely acknowledged that MLAT processes are too slow for rapidly developing counter terrorism and serious crime investigations. The UK's highly respected former Independent Reviewer of Terrorism Legislation, David Anderson QC, in his 2014 Report "A Question of Trust" said:

> *"There is little dispute that the MLAT route is currently ineffective. Principally this is because it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy. For example a request to the United States might typically take nine months to produce what is sought."*

Others have proposed relying on metadata, rather than content, to meet law enforcement's investigative requirements. This is not feasible. Although it is currently an important investigative and prosecutorial tool, metadata can never replace content. It can provide the "who, where, when and how" of a communication, but not the "what". The content of communications, including its "live" interception, is essential to ascertaining intent, location and imminence of a threat.

UK Investigatory Powers Framework

Privacy is at the heart of the UK's investigatory powers regime. The Investigatory Powers Act strictly limits which authorities can use investigatory powers, imposes high thresholds for the most intrusive powers and sets out in unprecedented detail the safeguards that apply to material obtained under the Act.

It contains an over-arching privacy clause which makes clear that warrants or other authorisations should not be granted where information could be reasonably obtained by less intrusive means. It also requires persons exercising functions under the Act – including Government Ministers and the new Judicial Commissioners – to have regard to the public interest in the protection of privacy, the public interest in the integrity and security of telecommunication systems, as well as other principles that underpin the legislation.

The UK does not believe the type of Bilateral Agreement sought here should require countries to have identical legal frameworks. What is important is that there are shared high standards of authorisation, transparency, privacy protection and oversight. The UK's laws reflect the view of the British people and Parliament. These will, like all countries, reflect our history, values and political system. The Act recognises both the importance of independent judicial authorisation and that Ministers are also accountable to Parliament for the actions of the Executive. This is important to the UK as a parliamentary democracy.

UK Agencies and Law Enforcement are governed and overseen by one of the world's most robust and transparent legal frameworks, which ensures adherence to strict principles of necessity and proportionality. The Act restricts the power to seek interception warrants only where it is **necessary and proportionate** for the prevention or detection of serious crime or in the interests of national security.

The Act and its Codes of Practice set out strong overarching principles that will apply, including:

- **Authorisation:** The Act overhauls the way that the use of investigatory powers is authorised. Warrants must be subject to a new "double-lock", so that they cannot be issued until a minister's decision to do so has been approved by a senior judge. At every stage of the authorisation process, necessity and proportionality must be tested.
- **Oversight:** The Act creates a world-leading oversight regime, led by a single new independent Investigatory Powers Commissioner with the resource and remit to oversee use of all investigatory powers set out in the Act. Lord Justice Adrian Fulford, one of the UK's most senior and respected Appeal Court judges, has recently been appointed as the first Investigatory Powers Commissioner.
- **Transparency:** The Act brings together powers already available to UK agencies in one clear and understandable piece of legislation. It imposes

requirements for regular reporting to the public and Parliament on the use of investigatory powers.

- **Necessity and Proportionality:** The Act strictly limits when investigatory powers can be used.

Specific safeguards set out in the Act and its associated Codes of Practice include protection for certain sensitive professions or categories of information, including Parliamentarians, journalists and material subject to legal privilege.

Conclusion

Amended US legislation and a UK/US Bilateral Agreement on Data Access will demonstrate that countries can work constructively with industry to overcome jurisdictional conflicts and that practical steps to improve public safety can be taken with due regard for transparency, online freedoms and the rule of law.

Congress now has the opportunity to set new global standards for cross-border data access, improve UK and US ability to protect each others' citizens and tackle global threats, through introducing and advancing this ground breaking legislation. The UK Government stands ready to assist in this important work and hopes that Congress can pass relevant legislation as a priority in 2017.