*Speech delivered by Deputy Assistant Attorney General Richard W. Downing June 20, 2022, at the German Parliamentary Society, Berlin, Germany, at an event titled, “Digital sovereignty in a transatlantic context - rationality versus political “ghost driving””*

Thank you for the invitation to present to you today. I appreciate the opportunity to be able to share my thoughts with so many esteemed and thoughtful colleagues.…

I would like to focus my remarks today on three points: First, the critical importance to criminal justice systems in democratic countries of the ability to access digital evidence located abroad; second, the sovereignty and other issues it raises; and finally, I would like to challenge what are perhaps some of your assumptions about what kind of regime would be required so that transborder access can take place with full respect for privacy and the rule of law.

In my official duties, I serve as the Deputy Assistant Attorney General in the Criminal Division of the U.S. Department of Justice, where I oversee teams of prosecutors and investigators who investigate cybercrimes like ransomware and child exploitation online. Digital evidence is critical to our ability to solve these crimes and successfully prosecute those who committed them. In addition, cybercrime can have enormous real-world consequences. Last year, a ransomware attack targeted a company that operates a pipeline that supplies nearly half of the fuel for the East Coast of the United States. This disruption to our critical infrastructure created a real change of thinking in the U.S. Of course, we have seen damaging attacks before – but few felt personally affected. This event disrupted distribution of fuel to millions. It brought home to leaders in government and industry alike the very real impact these criminal attacks have on the world. Similar ransomware attacks targeting hospitals and other institutions and infrastructure have been of great concern in both Europe and the U.S.

And of course, it is not just “cyber” cases that require digital evidence. The need for data about communications or stored on phones or computers spans every type of crime – from terrorism, to drug distribution, to organized crime, to child sexual exploitation, to fraud. In sum: there can be no dispute that the United States and Europe both need effective tools to gather electronic evidence – no matter where in the world it is stored – so our investigators and prosecutors can do their jobs of identifying the perpetrators, punishing the guilty, and deterring future wrongdoing.

To begin to provide for effective tools to combat cybercrime, about 20 years ago democratic countries came together to negotiate the Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention. In the succeeding years, the Budapest Convention has become the world’s leading multilateral cybercrime treaty with 65 Parties from around the globe, including 26 of 27 EU Member States, the United States, Argentina, Canada, Japan and Australia. Among the measures agreed to in the Budapest Convention was a requirement that each Party’s government establish the power to compel any communications or cloud providers located in its territory to disclose for criminal cases electronic evidence within its possession or control, regardless of where the provider might choose to store that data. The reason for this requirement was clear: Absent such a rule, law enforcement investigations could be thwarted by domestic companies merely renting server space abroad or using cloud-based services that store data outside the country. So important was this power to the effective investigation of criminal cases that every Party to the Convention was obligated to have it.

But while countries wish to have the power to reach out beyond their borders for evidence vital to their criminal cases, they also are understandably wary when other countries try to access data stored within their territory, or sensitive data they store in the Cloud. The natural impulse in such situations is for a government to try to block other governments from obtaining data located in its territory, an impulse which may be driven by a desire to protect privacy or fears that sensitive business or government data may be accessed. In Europe, such concerns have given rise to legislation such as GDPR at the EU level, and SecNumCloud in France, which seek to prevent access to data based on a foreign government’s compulsory powers.

The United States too has laws that impose potential restrictions on disclosure of data by providers in response to foreign compulsory orders, and these limitations can admittedly make it more difficult for even our most trusted international partners to access vital evidence of criminal wrongdoing. Accessing data located outside of a country is thus a two-edged sword. There is an inherent tension: the more countries pursue protection of privacy and build barriers to enhance their “digital sovereignty,” the greater the cost will be to effectively protecting our people from crime and terrorism.

The key to answering this policy question of when to permit access is whether the data access will be accompanied by sufficient protections against misuse. And the difficult part of this is determining where the line should be drawn in deciding whether those protections are sufficient.

As democracies, the United States, Germany, and the European Union believe in a rules-based international order. We uphold democratic values and individual rights in carrying out our criminal justice functions: We have strong rules to protect the individual from the enormous powers the State wields when it investigates and prosecutes criminal offenses, both in order to avoid convicting the innocent, and to identify and deter government abuse. We also put in place strong rules to protect the privacy of personal information. Here in Europe, you call it data protection, but other rights respecting countries have also developed rules which we apply in ways that, while not identical to your rules, are equivalent to them.

But there are also countries that do not have such protections. Look no further than the authoritarian regimes in Russia and China, where the justice systems are corrupt, politicized, or both; the regime supports criminal groups when it is in their interest to do so; and where the default tends towards the government having on-demand access to data, with little oversight or consequences for misuse. Rights respecting democracies have every right to defend themselves against regimes that have the intent and ability to weaken their institutions and even enrich themselves in the process. Thus, in the same way that the United States and European Union share a common interest in being able to protect our societies by fighting crime, we share a common interest in countering threats emanating from authoritarian states.

Now if you agree with what I have said thus far, I would like to take you one step further, and ask you to reflect on what kind of system of safeguards is sufficient to justify a broader ability of rights respecting democracies to access the foreign-located electronic evidence needed so that their justice systems perform effectively, while at the same time protecting privacy and sensitive information, and thwarting incursions from countries that do not respect the rule of law.

I think we all have to recognize that up to now there are very different views on how to accomplish this, even between close allies like the United States and the European Union. We can’t ignore that there is a perception in Europe that on some level it must be wary of the United States. I hope the time has come when we can move past such perceptions, which can drive a wedge between partners at a time when the strength in our unity matters. But much more than that, I honestly believe that many of the current perceptions, and the arguments that underlie them, are not based on the facts, and therefore need to be rethought.

To give one very prominent example, the recent U.S.-EU agreement in principle related to Privacy Shield. The United States has undertaken to make significant reforms to its systems for gathering foreign intelligence. This should go a long way to demonstrating that the U.S. is committed to ensuring that intelligence agencies are subject to strict systems of accountability when they access data.

Moving to my area of specialty, criminal law, we often hear of the perception in Europe that a 2018 law familiarly known as the CLOUD Act, bestows enormous powers on the U.S. government to obtain data held by U.S. providers abroad without any safeguards. I hope to demonstrate to you that this is in no way the case.

Specifically, what if I were to tell you – in response to the assertion that the CLOUD Act permits the U.S. to obtain evidence held in the cloud without safeguards – that, as I mentioned, the U.S., like virtually every EU Member State, is obligated to have this power in order to be in compliance with its treaty obligations under the Budapest Convention; and that this power is exercised by the U.S. through a system of safeguards that may equal or surpass that of any other country? Are you aware that these safeguards: first, strictly limit the purposes for which data can be compelled; second, provide that if a warrant were ever to be sought, it would not be issued unless an independent and impartial judge were convinced that extremely exacting U.S. legal standards of proof and particularity support its issuance; third, that a provider can seek judicial redress challenging issuance of the government’s demands; and fourth, that prior to a federal prosecutor seeking to enforce an order, give the Department of Justice the opportunity to evaluate whether such action is appropriate with due regard for the equities of partner countries. And, lastly, are you aware that – even before the U.S. can seek data unilaterally, including “through the cloud act” - it is required to first use its mutual legal assistance treaty with Germany, thereby permitting Germany to refuse assistance should it desire to?

In view of these explanations, would you perhaps be less concerned than before that an immediate danger requiring urgent legislative and policy measures was at hand? My point is that decisions affecting our relations are currently being made based on assumptions that are not necessarily correct.

I would also like to tell you that – contrary to the idea that it is a danger – the CLOUD Act is beneficial legislation that establishes a new paradigm designed to benefit global cooperation and enhance security for our partner democracies, by permitting legitimate foreign law enforcement access -- all while protecting privacy and the rule of law. It is little understood that the very CLOUD Act that has given rise to the misconceptions about U.S. law I have just described provides this benefit. Analogous to the EU’s proposed e-Evidence legislation, the principal chapter of the Act authorizes the United States to enter into bilateral agreements with trusted partners that meet rule of law and privacy criteria, enabling the lowering of our respective barriers that might otherwise stand in the way of providers complying with lawful orders from the other country. In other words, both countries would agree to eliminate any blocking effect of their laws so that each country can more efficiently obtain the information needed to protect their societies. Each country would then be free to serve covered orders directly on providers in the other country, without having to go through the other government or the existing time-consuming mutual legal assistance process. And in exchange for these benefits, the U.S. and the partner country would enhance their commitment to protect privacy and uphold civil liberties and the rule of law.

The CLOUD Act is the first, and -- thus far -- only legislation in the world that offers to other rights-respecting countries a way to get more effective and efficient cooperation in obtaining a broad range of evidence in electronic form. Other countries may decide to meet these same objectives in different ways, but it is a serious attempt to solve the problem and it deserves serious consideration. We hope it will receive it, based on a thorough and honest evaluation of it, and not on innuendo.

I would like to conclude by reiterating: cross-border transfers of electronic evidence are necessary and appropriate, indeed they are a critical component of investigating crime in the 21st century. Cautiously, but also creatively, partner countries will have to find long-term solutions like the U.S. CLOUD Act in order to protect the public and their democratic way of life.

The United States has already entered into CLOUD Act agreements with the United Kingdom and Australia, and we hope to do so with the European Union and others as well. Our societies expect us to protect – at the same time – their security, privacy, and civil liberties. I think they are not asking for the impossible, and I do not believe these issues should divide us. With good will, flexibility to accommodate differences between national legal systems, and determination, we will arrive there, and our societies will be better for it.

Thank you for your kind attention.