LAWFUL ACCESS TO DATA:

THE US V. MICROSOFT CASE, SOVEREIGNTY IN THE CYBER-SPACE AND EUROPEAN DATA PROTECTION

WITH A STUDY BY THEODORE CHRISTAKIS,
PROFESSOR OF INTERNATIONAL LAW - UNIVERSITY GRENOBLE ALPES / INSTITUT UNIVERSITAIRE DE FRANCE - DIRECTOR OF THE CENTRE FOR INTERNATIONAL SECURITY AND EUROPEAN STUDIES - DEP. DIRECTOR OF THE GRENOBLE ALPES DATA INSTITUTE

DECEMBER 2017

ceis

THE CHERTOFF GROUP

FOREWORD

Microsoft and the US government have been arguing since 2013 over the validity of a mandate issued by a US judge on content data hosted by Microsoft in Ireland. The saga is soon coming to an end. In October 2017, the Supreme Court decided to consider the case that was brought to it by the DoJ, and should make a decision by June 2018. The crux of the matter is whether a US judge can, without going through the dedicated international cooperation processes, request data hosted on server located abroad.

The question is quite simple but the stakes are many, because each party tries asserting their own interests. For States, this is about ensuring their own safety by providing judicial authorities an easy access to digital data wherever located. In this regard, it is quite clear that existing arrangements based on MLATs - mutual legal assistance treaties – do not meet the exponential growth in requests for international mutual assistance on digital data, nor the necessary responsiveness required in the cyberspace. For businesses, be they users or cloud operators, it is about ensuring they have a powerful and cost-effective "IT energy" available to cope with digital transformation. This implies "massifying" their activities around a handful of large data centers, and avoiding conflicts of laws and jurisdictions. For both, it is also a question of maintaining and strengthening citizens-users' trust in the protection of their personal data, which is essential for the development of new uses.

The decision of the US Supreme Court will therefore carry a world of meaning. If the Department of Justice is proved right, US judges will ipso facto be given some kind of global jurisdiction: during a domestic process, they will be entitled to request content data - rather than merely connection data - to any operator on the planet. And without even claiming to an extraterritorial application of the law, since the DoJ regards that data as coming under US law as soon as they can be consulted from the US territory... A sleight of hand that potentially "territorialises" much of the world's data in the US, since data stored in the "cloud" is by definition accessible from any place on earth.

This would result in repeated infringements on the sovereignty of concerned States, in an incompatibility with European data protection agreements and legislation (and in particular the European Regulation on the Protection of Personal Data ...), and in permanent legal uncertainty for digital operators who will be facing a dilemma. All the more than other countries could also be tempted by unilateralism and could stop

using existing international law tools. The consequence would be a proliferation of conflicts over sovereignty and the exacerbation of digital protectionism, a situation with no winners. Only looking at data flows between Europe and the US shows how much Europe depends on the transatlantic relationship when it comes to digital. This is the case on both technological and economic levels. This is not about over-reacting and systematically raising the risk of the "balkanisation" of the Internet each time States "locate" or "relocate" certain type of data, even at the benefit of local digital players or local subsidiaries of US companies. This phenomenon, already well underway, is part of a perfectly legitimate quest for sovereignty. Even more so in a post-Snowden context...

Only a few months away from the decision of the Supreme Court, we believed it was essential to capture the ins and outs of this case, and to imagine solutions likely to reconcile States, business and individuals' interests. This is what this White Paper initiated by Microsoft and co-written by The Chertoff Group and Théodore Christakis, professor of international law and senior member of the Institut Universitaire de France, is all about..

Guillaume Tissier
General Manager CEIS

This white paper, prepared by The Chertoff Group in consultation with CEIS, reflects our concern with the growing disconnect between American and European approaches to cross-border exchange of data for law enforcement and counterterrorism purposes, and the accompanying issues of data privacy and security. We have been warning for some time about the potential adverse consequences from trends toward balkanization of the Internet.[1] Our hope has been, and remains, that enhanced cooperation between the U.S. and Europe can be fostered through greater understanding of the potential risks associated with the current path of policy development.

To that end, this paper is intended to highlight for our European counterparts a potential inflection point that looms – an appeal pending before the United States Supreme Court. Resolution of that matter has the potential to accelerate the deterioration of cross-border cooperation in significant ways. Yet the case, in our perception, has not received the attention it deserves in Europe nor generated the engagement we expected. We respectfully submit that this lack of attention is not in the best interests of Europe or America. This white paper summarizes the case, explains why its resolution is important, and suggests a way forward for European engagement.

The Chertoff Group

TABLE OF CONTENTS

MICROSOFT V. UNITED STATES: A CRITICAL INFLECTION POINT

by The Chertoff Group

As it returned from summer break in mid-October, the U.S. Supreme Court agreed to take up a case that may directly impact U.S.-E.U. data sharing activities – *Microsoft v. United States*.[2] The case will be argued early next year, and a final decision will be released before the Court takes its summer recess at the end of June 2018.

Broadly speaking, the case relates to a warrant issued by the U.S. government to *Microsoft* which, if enforced, would require *Microsoft* to repatriate content data held in an Irish data center to America for provision to law enforcement authorities. At issue is a simple legal question: May U.S. law enforcement authorities compel *Microsoft* to produce in the U.S. data held in an overseas data center? More prosaically: Does American law control data stored in Europe?

The resolution of that question is, or ought to be, of profound importance to Europeans. Data sharing between the U.S. and E.U. is vital to both government and industry, for both law enforcement investigations and for all types of commerce. And, given the nature of cloud architecture, data storage and transfer is now a global issue—physical borders are not determinative.

The globalized nature of the Internet has had an especially profound impact on law enforcement. Investigations of local crimes that were once restricted to the narrow geographic area where the offense occurred have

now, routinely, been transformed into cases where evidence gathering requests involve data that may be stored almost anywhere in the world. The content of communications relating to an offense, and the meta-data associated with that content, may be stored in multiple locations and in some cases, move among data centers for any number of reasons, both technical and practical. Because data is no longer localized, law enforcement must often, in effect, cross national boundaries to investigate even the most routine of cases.

In the U.S. and in Europe the processes for these cross-border law enforcement efforts often are grounded in outdated laws and policies. The Mutual Legal Assistance Treaty ("MLAT") process for transnational criminal cooperation is both cumbersome and fraught with legal uncertainty. Requests made through the MLAT process often take months, and in some cases years, making it a source of frustration for law enforcement authorities on both sides of the Atlantic.[3] As a result, under the understandable pressure to deal quickly and effectively with criminality, law enforcement in America has turned, systematically, to the much more rapid process of issuing domestic warrants – but with the resulting challenge that they are, in effect, demanding that American companies give extraterritorial, overseas effect to American law enforcement demands. This practice raises the fundamental issue of sovereignty and leads to conflicts of law and questions of international comity.

Precisely this legal question is now pending before the U.S. Supreme Court which will consider the validity of a domestic warrant issued to *Microsoft*. A decision affirming the government's authority to issue such a demand would commit the U.S. to the position that its demands for the production of evidence can be given extraterritorial effect. That, in turn, will have significant impact on U.S.-European cooperation.

Unilateral "Solutions" And Their Consequences

In an era of heightened cyber-criminal activity and election interference, trans-Atlantic cooperation on cyber-crime and cyber-attacks is more important than ever. Yet without broader legislative action and/or international agreement, a decision in favor of the government in the *Microsoft* case will likely have the perverse effect of making trans-Atlantic cooperation more difficult for law enforcement, government, and businesses. The Extraterritorial application of law will, in our judgment, negatively impact cooperative efforts between the U.S. and other countries and trench upon their sovereignty.

To see why this prospect is so fundamentally disruptive and daunting, it is useful to indulge in a thought experiment – what will law enforcement data sharing look like if the U.S. government's view on extraterritoriality prevails? The picture is not a pretty one and we can already see the outlines of it taking shape in the actions of various nations. Looking into potential impacts, we see several areas in which international cooperation between the U.S. and Europe is nearly certain to suffer.

These impacts are likely to include:

1) Reciprocal extraterritorial application of the domestic law of other nations to assert the right to access data held within servers under American jurisdiction, creating conflicting and incompatible legal obligations for providers;

2) Expanded, and what could be described as greatly enhanced, data localization requirements in non-American countries designed to prevent U.S. law enforcement from accessing data relating to their citizens;

3) Perhaps most troubling, likely adjustments to Privacy Shield or, even, the elimination of mechanisms that allow for companies to transfer data across the Atlantic. Surely these prospects are appealing to no one.

Conflicting and Inconsistent Legal Obligations:

First, one of the major problems posed by the U.S. government's position in *Microsoft* – if other countries take the same path, is that it changes a cooperative law enforcement environment to one in which competition predominates. We are confident that if the Court upholds the U.S. assertion of extraterritorial application of its laws in order to ensure access to data, other countries will quickly do the same. Indeed, that trend is already evident.

For example, Brazil recently arrested a local executive from a U.S. technology company because they refused to turn over data stored in the U.S. Brazil issued a local warrant that was apparently in conflict with an American prohibition.[4] Similarly, in the United Kingdom, the government has adopted the Data Retention and Investigatory Powers Act which, by its terms purports to have extraterritorial application.[5] And, even in Europe, the trend is growing. Recently, the Belgian Supreme Court fined Yahoo for failing to comply with a court order that was maintained outside of Belgium.[6] The goal, as we've said, is understandable; the current MLAT process is inadequate. But to understand the motivation is not, necessarily, to support the result.

If the *Microsoft* matter is decided adversely to *Microsoft*, we can only imagine that the situation will get worse, rather than improve. At its most basic level, by enshrining successful unilateralism into American law, the Supreme Court would be disincentivizing international cooperation in favor of independent action. What incentive would the U.S. have to engage the international community on law enforcement access to data if U.S. law enforcement was able to leverage U.S. legal process to obtain access to the data that they need? We have no doubt that, faced with such a decision, European countries will respond to the U.S. by applying their own laws extraterritorially to European corporations and citizens. Indeed, if unilateralism becomes the norm, then national authorities will have almost no reason to act with reciprocal respect for each other's interests.

In the end, this trend will create a proliferation of conflict of law problems, creating conflicting and inconsistent legal obligations for providers. And, not least, this approach will encroach on the fundamental value of sovereignty which is challenged by overseas enforcement of another country's effort to compel production of data. Whose law applies in what case if every country is able to apply its law extraterritoriality? How do governments and courts resolve these conflicts of law? Which country's law should a provider follow in what case? In such an environment the distinction between international and domestic law will lose meaning and the result will be a legal free-for-all where the only determinant will be the exercise of raw power that can be used to compel a particular result.[7]

Again, while it is easy to see the contours of how this will happen and why it may seem justified to the sovereign actors, at the higher level of asking

"what is best for the global community?" it cannot be the right answer. The rule of law depends on a law of rules – a domain where relative certainty and consistency abides. Radically indeterminate conflict of law determinations undermines this fundamental value. It will also, have the secondary effect of, again, undermining cooperation between U.S. and European law enforcement, leading them to pursue data through their own courts rather than work together.

More Restrictive Data Localization:

Second, and perhaps most likely, we think that if there is a pro-U.S. government result in *Microsoft*, trends toward data localization will almost certainly accelerate, likely to the point of what one could term "extremely restrictive data localization." European countries, in particular, are likely to pursue data localization requirements to prevent perceived harm to their citizens. This is, also, an understandable impulse – an enhanced version of data localization is one of the only ways to ensure that a country's law applies to the data of their own citizens by requiring it to be held domestically by a provider who will comply with local law.

This would be a step beyond existing data localization regimes, which are generally limited to a requirement that data on local citizens be physically stored within a country's borders without regard to where else the provider operates. If the Supreme Court were to accept the government's argument, U.S. authorities would be able to compel any service provider with a presence in the U.S. to turnover data regardless of where it is stored, which would render existing data localization requirements inadequate. In response, countries would be incentivized to create far more restrictive data localization requirements that require the provider to only operate within the domestic jurisdiction in question, thereby preventing authorities in other countries, such as the U.S., from using the provider's presence in their country as grounds to compel them to turn over data under an extraterritorial application of their own laws.

But this sort of highly restrictive data localization, however, understandable, is a second-best solution. For one thing, it is effectively cyber protectionism – privileging local providers over global ones in a way that ultimately disserves the domestic consumer. More importantly, it would result in the creation of an extremely balkanized internet in which providers operate within a single country and are obliged to avoid cross-border activities in order to avoid extraterritorial application of domestic laws. The global internet would become more of an idea than a reality. Whichever answer one prefers, it is simply an untenable argument to suggest that sovereign disagreements on policy should be resolved at the price of reducing the internet to loose patch work of local internets designed to ensure compliance with local law.

Changes to Privacy Shield and Similar Data-Transfer Mechanisms:

Finally, in a post-Microsoft world, we will likely see collateral effects in the commercial sector. If European authorities do not believe that they can trust U.S. law to respect E.U. law, then, generically, they will be more reluctant to permit European personal data to be transferred to the U.S. This is a necessary corollary of the trend towards extreme data localization that will likely lead the E.U. to seek adjustments of Privacy Shield and other mechanisms that allow for the transfer of the personal data of E.U. citizens to America.

For good reason, we anticipate that post-*Microsoft* (if the U.S. government prevails) the E.U. will perceive privacy guarantees offered through Privacy Shield, Binding Corporate Clauses, or other mechanisms to be unenforceable against government action and thus of less value. Further, such a decision by the Court will probably be seen as a clear indication that the U.S. doesn't value foreign laws or personal privacy to the same degree as Europeans. An adverse *Microsoft* decision may also influence the European Court of Justice as it continues its consideration of challenges to Privacy Shield. In the end, cancellation of Privacy Shield would be disruptive to businesses in the U.S. and E.U.—if these mechanisms are eliminated or significantly modified it would be effectively impossible for companies to move data between the two jurisdictions. This would, manifestly, have a significant economic impact, making it deeply problematic for many businesses to operate in both jurisdictions in a unified manner.

In sum, the post-*Microsoft* world in which the U.S. government wins suggests that any victory would be a pyrrhic one that disadvantages the United States and also has severe adverse impacts in Europe. That prospect is precisely why Europeans with interests in these issues should consider enhancing their dialogue with their U.S. counterparts now, before this dystopian future becomes reality.

A Proposal for Engagement

Rather than accept this grim future as inevitable, Americans and Europeans should be seeking out opportunities to collaborate on lawful access and build a system that both respects sovereignty concerns and enables effective enforcement while protecting citizen privacy. Though ambitious, the goal is not impossible to achieve. The U.S. and Europe should be able to reach consensus, through international diplomacy and agreement, on how law enforcement gains access to data stored abroad—our values are fundamentally the same. Indeed, agreement between the U.S. and European countries is critical if we hope to build international norms that align with our values—such an agreement can help lead the way for other countries and form a broad basis for global consensus.

The question, then, is how to get to a place of agreement, especially as the *Microsoft* decision that may disrupt the effort looms.

To begin with, Europeans should consider the implications of the *Microsoft* case and determine their interests in the broader issues. Now is the time for Europe to engage on these issues and make their voices heard within this debate – later may be too late.

The Supreme Court is unlikely to understand the global implications of its decision if those are not brought to its attention by competent authorities who understand the problem. In addition to explaining, clearly, what the potentially adverse consequences would be, Europeans should also, in our view, be open in their commitment to a dialogue with the U.S. government. In the midst of legal ferment, the Court should consider the possibility of a way forward to achieving a trans-Atlantic consensus on what the legal framework and solutions to these issues should look like. In other words, the Court should be aware: **a)** that decisions about trans-Atlantic law enforcement cooperation should be made jointly and not by a single U.S. court; and **b)** that the prospects for a potential solution is realistic, and not just a pipe dream.

Happily, there are a number of areas of progress that can be pointed to as reasons for optimism that a mutually acceptable solution is in the offing. Indeed, the U.S. Congress continues to debate a variety of potential solutions. Various other organizations and companies are working on ways to address at least some of the problem.

For example, in the U.S. Congress, active consideration is being given to the bipartisan proposal to enact the "International Communications Privacy Act" – a proposal that would, in effect, end American unilateralism in return for reciprocal commitments from our allies. Congress and the Executive Branch are also considering the first-of-its kind bilateral agreement between the U.S. and the United Kingdom.[8] This proposal amounts to a mutual recognition of the adequacy of each others' legal process, directly addressing potential conflicts of law while ensuring the preservation of sovereignty for both countries. This agreement is seen as a potential model for additional bilateral agreements between the U.S. and European countries.[9] Meanwhile, civil society groups in the U.S. and the E.U. are engaged in extended efforts to articulate broadly agreed upon norms of behavior that could be generalized into an agreement of lawful access and data sharing.

While none of these efforts has yet to reach fruition, each holds promise. More to the point, each has the advantage of being derived from a broadly representative base that reflects the views of all stakeholders. While we have no crystal ball to predict how these efforts will eventually resolve, we are confident in predicting that each and every one of them has a better chance of leading to a stable, non-unilateral, global system

of data exchange than would the exercise of U.S. legal imperialism by the Supreme Court.

In the end, the core concept that must undergird our joint efforts is trust. Extraterritorial application of domestic law, data localization requirements, and protectionist practices undermine trust. So, to, would a unilateral expression of law by the U.S. Supreme Court. Countries need to retreat from autonomous action on these issues and work to build that trust.

A first step – a vital step – in that process is for our European colleagues to share their views on these issues with their counterparts in the United States. The U.S. legal process badly needs to hear the European perspective as it considers the issues before it in *Microsoft*. It may not be sufficient to persuade the Court, but left unexpressed it will surely have no influence at all.

Conclusion

If the Supreme Court concludes that U.S. warrants can operate extraterritorially, that decision will have a major impact on cooperation between the U.S. and E.U. on issues of law enforcement and counter-terrorism cooperation. One nearly-inevitable consequence will be the pursuit of unilateral solutions to individual parts of the problem. But, that result isn't a solution – in fact, it makes finding a solution harder and has negative consequences.

Solutions will be difficult, but many are already working to find them. Finding them depends on international cooperation and trust—trust that would be undermined by a Supreme Court decision in favor of the U.S. government position. We urge Europeans to consider the long-term impacts of their actions when addressing these issues today—unilateral, short-term fixes are damaging the chances of identifying more effective, long-term solutions. Now is the time for the U.S. and Europe to engage in a meaningful dialogue that addresses these vital issues, working toward an international agreement rather than unilateral solutions.

Références

[1] See Michael Chertoff, "Wanted: An International Rule of Law for Cloud Data," The Wall Street Journal, December 18, 2014, Available at https://www.wsj.com/articles/michael-chertoff-wanted-an-international-rule-of-law-to-govern-the-cloud-1418946310.

[2] The formal case title is In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197 (2d Cir. 2016), reh'g en banc denied, 855 F.3d 53 (2d Cir. 2017), cert. granted, __ U.S. __ (Oct. 16, 2017).

[3] Andrew K. Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Age (Washington, DC: Global Network Initiative, January 2015): 3, Available at https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[4] Jonathan Watts, "Brazilian police arrest Facebook's Latin America vice-president," The Guardian, March 1, 2016, Available at https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan.

[5] Daniel Severson, "Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill," Lawfare, March 14, 2016, Available at https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill.

[6] Stibee, "Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies," Lexology, July 15, 2014, Available at https://www.lexology.com/library/detail.aspx?g=065e35f1-5e2d-4f9d-9200-e236fcbb9397.

[7] A related impulse could be seen in the efforts by some data protection authorities to apply European data protection law extraterritoriality. The most notable example thereof is the French DPA's effort to require Google to apply delinking decisions globally. Here, too, the motive is understandable and the mechanism is similar. This issue remains a point of disagreement between the U.S. and Europe.

[8] David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests," Lawfare, July 16, 2016, Available at https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests.

[9] Joe Uchill, "DOJ pitches agreements to solve international data warrant woes," The Hill, May 24, 2017, Available at http://thehill.com/policy/cybersecurity/335015-doj-to-sens-bilateral-agreements-could-solve-international-data-warrant.

DATA, EXTRATERRITORIALITY AND INTERNATIONAL SOLUTIONS TO TRANSATLANTIC PROBLEMS OF ACCESS TO DIGITAL EVIDENCE

LEGAL OPINION ON THE CASE MICROSOFT IRELAND (SUPREME COURT OF THE UNITED STATES)

by Théodore CHRISTAKIS

Professor of International Law
University Grenoble Alpes/ Institut Universitaire de France
Director of the Centre for International Security and European Studies
Dep. Director of the Grenoble Alpes Data Institute

1. Context and objectives of this study.

The author was contacted on 17 November 2017 by CEIS to prepare a legal opinion on the "*Microsoft Ireland Warrant*" case between the US government and Microsoft before the United States Supreme Court. This legal opinion will be integrated into a "white paper" on this case, launched by Microsoft and published by CEIS, the Chertoff Group and the author of this study. The author has enjoyed complete independence in the drafting of this study. The contents of the study are not binding on CEIS, the Chertoff Group or Microsoft and exclusively reflect the opinions of its author. Part I of this study presents the parameters of this case in the most accessible way possible. Part II examines the issues raised in the US Supreme Court. Part III assesses the negative consequences that a decision of the Supreme Court in favour of the American government might have. Part IV, finally, shows that international law offers States various ways to find solutions to the problem of access for law enforcement services to digital evidence during a criminal investigation.

2. Avoiding confusion in a complex affair.

The *Microsoft Ireland* case raises fundamental questions about the legal status of data in the contemporary world and the sovereignty of States in cyberspace, issues that are of interest to the public authorities in various nations as well as to businesses, individuals and civil society. The implications of this case should not be underestimated by anyone. At the same time, the case is complex. Its meandering and extensive ramifications could easily mislead the observer and induce him into logical errors or unfortunate comparisons. It is therefore imperative to "simplify" this case as much as possible by presenting its ins and outs, as well as the real legal issues it raises.

3. Facts.

In December 2013 a US Judge ordered Microsoft to submit to the US authorities, in the context of a drug trafficking case, the emails of a suspect which were stored in a Microsoft server located in Ireland. The search warrant for this email account was given by the Judge under the US Stored Communications Act of 1986 ("SCA"). Microsoft, however, refused to submit the contents of this email service on the grounds that the data in question was in its *data centre* located in Ireland and that the SCA had no extraterritorial effect. In a ruling issued on July 14, 2016, the US Court of Appeals for the Second Circuit ruled that the US government could not force a company to submit emails from its clients present on servers located outside the United States. The Court found that Congress had not given the provisions of the SCA Act extraterritorial application and that a warrant under that law could apply only to data stored in the United States. The US government challenged this decision in the US Supreme Court, which in October 2017 agreed to take up the case. The proceedings are currently underway and a decision is expected in June 2018.

4. What is at stake here: "content data".

First, it should be noted that what is at stake in this case is the US government's access to the "content data" of a Microsoft client, in this case the content of all emails that the suspect has exchanged with other persons. This is important for the understanding of the case for several reasons. **First**, because "content data" (emails in this specific case, but it could be any documents, photos or movies stored by a suspect in the cloud) are at the heart of privacy, both for the persons directly involved and for third parties (whether they are the suspect's correspondents, whose emails exchanged with the suspect will also be read by the authorities, or, in other cases, persons appearing on images and films). **Secondly**, because the demand put by the US authorities to Microsoft, which is for unilateral access (and without going through the international mechanisms of mutual legal assistance provided for that purpose) to the "content data" of one of its clients, distinguishes this case from the many which concern requests made by States to suppliers for access to mere "subscriber information" - that is, information which only makes it possible *to identify the user* of a specific IP address or service (without having access to the content of his communications). In practice, States frequently ask ISPs (Internet and Cloud Service Providers) for the release of "subscriber information" in the context of investigations, and ISPs usually provide it (if they consider that the request is formulated in a legal framework by a country respecting the rule of law).[1] The demand to produce "**subscriber information**" is obviously less intrusive to human rights and the interests of third parties than the US government's request for access to "content data" in the *Microsoft* case. Moreover, with regard to "subscriber information", States could eventually rely on article 18.1.b of the Budapest Convention on Cybercrime of 2001 allowing them to adopt legislation ordering ISPs to disclose "subscriber information" (and *only* such data) after an injunction from the authorities and this irrespective of their place of storage. The *Microsoft Ireland* case therefore has nothing in common with cases (like the "Twitter" case in 2013 in France[2]) where the ins and outs are entirely different and relate only to access to "subscriber data".

5. The principle advocated by the US government would make it possible tomorrow to obtain electronic messages, stored in France, of a French citizen and resident of France.

The second important element to consider is that the nationality of the suspect *has not been communicated* to the court by the US authorities. In his separate opinion, Judge Gerard Lynch emphasised that: " If he or she is Irish (as for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland".[3] What Judge Lynch points out in this case is that *the principle* at the root of the Microsoft case should be of interest to all States. If the Supreme Court finds in favour of the US government, that means that, tomorrow, the US authorities could, for example, issue a mandate requiring Microsoft or another cloud provider operating in the United States (Apple, Amazon, IBM, Google, Facebook etc.) to submit the "content data" of a French national suspected of a crime in the United States (including, for example, a journalist accused of undermining US national security), even though this French citizen lives in France and his data are stored by the relevant supplier in France, and this without using an international request for legal assistance or any other form of cooperation with the French authorities.

6. The place of storage of the data is known: Ireland.

Another important aspect of this case is that the place of storage of the data was immediately communicated to the US authorities by Microsoft, which gives an assurance, moreover (see §15), that it is always able to indicate to the authorities where the data associated with a specific account they are looking for are located. Whatever legal considerations one might have in the event that an ISP could not know and/or communicate the place where the data are located[4] these issues are irrelevant to the *Microsoft Ireland* case. In other words, in this case, the United States *knows* to which competent authority the request for mutual legal assistance is to be made and is perfectly able to approach Ireland with the virtual certainty of obtaining the data in what the former Irish Minister of Justice said should be, depending on the emergency, "a matter of weeks" or even just "a matter of days".[5] However, the United States has not made use of the mutual legal assistance mechanisms, opting rather for a unilateral approach by ordering Microsoft to submit these data.

7. Access to electronic data is crucial for law enforcement and police services.

Both the US government and Microsoft agree on a preliminary point, which would be accepted by any State: Technological developments and the "digitisation" of people's lives present a huge challenge for law enforcement and justice, which, in order to effectively do their job and protect society, must secure the evidence on servers. Beyond "cybercrime", evidence related *to any type of offence* will be stored on computer systems that are often located abroad. In order to effectively investigate and secure evidence for legal proceedings, law enforcement agencies must access "evidence in the clouds". This applies as much in the fight against terrorism and it's financing as for a whole series of other crimes such as fraud and financial offences, money laundering, murders, assaults and other violent crimes, human trafficking, drugs trafficking, child pornography and other forms of abuse against children. Both the US government and Microsoft agree that it is necessary to ensure the rule of law in cyberspace and find solutions that allow the authorities access to digital evidence. They differ, nevertheless, on how to achieve it and how to resolve the many legal and jurisdictional challenges raised by this problem.

8. The SCA Act has no extraterritorial effect.

A second point that both parties seem to agree on is that the SCA, on the basis of which the injunction was granted (§3), cannot apply extraterritorially. The United States Government has in fact acknowledged, on several occasions, that "*It is undisputed that* [the SCA] *lacks extraterritorial scope*".[6] The Court of Appeals also concluded that " Congress did not intend the SCA's warrant provisions to apply extraterritorially"[7] and the majority judges even called on Congress to "revise a badly outdated statute"[8] written well before the era of email and the cloud - a process which is currently underway, as a proposal for a law entitled "International Communications Privacy Act" (ICPA) was introduced before the US Senate in 2016.[9] The points of agreement between the parties stop there, however.

9. Is there "extraterritoriality" in this case?

One major point of disagreement is whether this case involves an extraterritorial application of the SCA. If we are indeed dealing with a context of extraterritorial application, the Court should then agree with Microsoft. The limited space of our study does not allow us to go into the details of the subtleties of American law discussed by both parties - and especially the difference between a "warrant" and a "subpoena" which, in any case, does not contribute anything to the international understanding of this case and its important implications. Let us therefore attempt to simplify. **For Microsoft** (and the Court of Appeals) matters are simple: a SCA mandate cannot apply to data stored in Ireland as it cannot have extraterritorial effect. This extraterritorial effect is clearly present in this case. If the US government wishes to access this data, it can only make a request to the Irish authorities in the context of the existing mutual legal assistance mechanisms. **For the US government** on the contrary, there is, in this case, "*no extraterritorial application* of the law". According to it, from the moment the data in question are accessible from the United States (even if they are stored in Ireland), the entire case is taking place on American soil and so there is no "extraterritoriality" (prohibited under the SCA). The Government emphasises in this regard that: *"Microsoft's U.S.-based employees could make that disclosure without leaving their desks"*.[10] A click of the mouse from Washington DC is enough to access the data. For the US government, this transfer of data by Microsoft from Ireland to the United States does not imply any invasion of the privacy of the suspect. It is only at the moment of "*disclosure*", that is, when the US government agent opens emails transferred by Microsoft to the United States that there is invasion of privacy (albeit justified because it is a criminal investigation). Since this "disclosure" takes place in the United States, only US law is applicable, to the exclusion of any foreign law relating to the protection of privacy. The fundamental question that the Supreme Court must answer is therefore relatively simple: *is the request made by the US government to Microsoft an "extraterritorial" application of the law on which that request is based?* **For the US government** *the answer is negative because the only relevant criterion is the place from where the data is accessible*. Since Microsoft (like the suspect himself indeed) can access this data from the United States, everything happens on American soil. **For Microsoft**, on the other hand, *the decisive criterion is the place of storage of the data*. As long as this data is stored in Ireland, the US government is clearly asking Microsoft for an action that is extraterritorial in scope.

10. Necessity makes law?

Another issue raised by this case, which seems to be the subject of major disagreement, is whether the need for law enforcement agencies to access evidence in the cloud to do their job and protect society (§7) is a sufficient reason for the Supreme Court to confer this legal option on the government. In its submission, **the government** accuses the decision of the Court of Appeals rendered in 2016 in favour of Microsoft of constituting an "*unprecedented ruling [which] has put the safety and security of Americans at risk by severely limiting a critical law enforcement tool*". The case is presented as asking a question "of exceptional importance to public safety and national security".[11] The message to the Supreme Court is clear: the end justifies the means. For **Microsoft**, however, this shortcut is not acceptable. According to it, the request for access to "content data" stored in a foreign country poses considerable risks, both for the individuals concerned (invasion of their privacy and even other rights, as we shall see in §21 and 23), for the companies themselves (which could, in particular, be in a situation of conflict of laws and jurisdiction - §24) and for the States concerned. According to Microsoft, therefore, necessity must be managed *within* the framework of established law - and by improving this framework, but not unilaterally and anarchically. This position seems compatible with the premises of contemporary international law. As we have explained at length elsewhere, the need is *taken into account* by the law but it is also strictly circumscribed by it to avoid risk of abuse.[12]

11. The relevance of international law.

This brings us to a final point. Whereas Microsoft's submissions also take international law into account, those of the US Government do so only to a lesser extent (which is consistent with the main argument that "everything occurs in the United States"). The Court of Appeal only devotes one paragraph of the 43 pages of its decision to international law (*below* §17) and it is probable (though regrettable) that the decision of the Supreme Court will not include even one. Yet this case is of direct relevance to international law. If, from the point of view of US law, the question is: "is there or is there not, in this case, an extraterritorial dimension?", from the point of view of international law the question is whether this extraterritoriality is problematic and what might be the effects of this case for the international legal regime. In the rest of this study we will therefore also address these issues.

II. The clear existence of an element of extraterritoriality (and the problematic criterion of "where the data is accessible from")

12. The concept of extraterritoriality in international law.

Before answering the question of whether the mandate adopted on the basis of the SCA includes an element of extraterritoriality (in which case the Supreme Court should rule in favour of Microsoft by upholding the decision of the Court of Appeals), it should be briefly discussed what this term actually means. International law confers on the State the legal power to subject natural and juridical persons, activities and property to its legal regime. State jurisdiction is divided into legislative power (the power to issue norms, also called "prescriptive competence"); judicial jurisdiction (administration of justice to deal with the breaches of the rules – also called "adjudicative competence"); and executive or enforcement power (power to give effect to orders emanating from its legal system through tangible and if necessary forcible actions). The big question is: where the State can exercise these different powers. According to international law, the State can exercise all these powers within the limits of its territory - this is called the "territorial" jurisdiction of the State. *The State* may also, but under certain conditions, exercise its jurisdiction over persons (especially its nationals) or property situated *in the territory of another State*, or even in spaces belonging to no State (such as the High Seas). This is called "extraterritorial jurisdiction". The latter is, of course, strictly governed by international law because it goes without saying that the will of a State to exercise its powers (especially executive) on the soil of a third State could violate the sovereignty of the latter and create strong international tensions. It can thus be said that, in general, there is extraterritoriality in the application of a norm "if all or part of the application process takes place outside the territory of the State which issued it" or whenever "a State aspires to intervene, through its legal regime, in matters situated outside its territory".[13]

13. The logical impasses of the "where the data is accessible" criterion.

We have seen that the US government considers that there is "no extraterritoriality" in the *Microsoft Ireland* case because "the data is accessible from the United States". This argument may seem at first logical and reflect a profound transformation of the concept of [extra] territoriality in the digital world. It is, in fact, highly problematic, for several reasons. First of all, and since virtually all digital data is "accessible from the United States", the SCA would apply to all data in the world: those of Americans, but also those produced by foreigners abroad and stored abroad. In other words, even if there is no link between the suspect and his data, on the one hand, and the United States, on the other hand (other

than the existence of a warrant adopted by the US authorities), the case would still be thought to be happening in the United States (because the data is accessible from US soil). Thus, even for a French person resident in France, who has never set foot in the United States, using a mail server storing his data in France, there would be "no extraterritoriality element" in such a request addressed to his ISP (having its headquarters or a subsidiary in the United States) to access his emails on a US mandate because "he could have access to his mail from a computer in the United States". The SCA, which everyone recognises as having no extraterritorial effect, could miraculously be applied to access the emails, photos and personal documents of virtually any individual with a cloud account that can theoretically be consulted from the United States! The fallacy of the argument seems too obvious to dwell on. As for the attempt to "sequence" the operations (§9) by claiming that there are two distinct operations: 1) the "transfer of data by Microsoft to the United States and 2) the moment of "disclosure" to the authorities of this now "American" data" - it is equally misleading. We do not have the space to dwell on this last point, but the extraterritoriality is obvious to the extent that the transfer of data to the United States was only performed because the mandate *constrained* Microsoft to do this and to transmit this data to the US authorities. It is therefore impossible legally and logically to "salami-slice" these operations.

14. The limits of the campaign against the criterion of "the place of the storage of data".

This brings us to a key question: does Microsoft's "location of data storage" criterion have any validity? The US government has been very insistent on the "arbitrariness" of such a test. Data is extremely mobile and fluid: it moves all the time and it is everywhere. Cloud providers themselves concede that they store data not at one location but in multiple locations (making the copies necessary to avoid data loss if there is a problem with the main *data centre*) and that they make the data travel whenever a maintenance operation requires it. The location of the data could be decided exclusively on the basis of economic considerations and change if less expensive options arise. How is it possible to deprive the courts of access to the data necessary to do their job on the basis of such a questionable, fluctuating and arbitrary criterion? Why subject the State authorities to the torment of Tantalus, forcing them whenever

the data has "moved", to launch new, costly and time-consuming mutual legal assistance proceedings in new countries of "storage"? Is there not a risk that "digital paradises" will appear in unscrupulous countries with the complicity of some ISPs who systematically move the data to them to prevent justice from reaching it? All these arguments are important and could lead to endless debates. This is why the author of this opinion is convinced that the criterion of the location of the data is only one of many criteria to be taken into account in order to build a satisfactory legal regime (*below* §28). However, these arguments should not lead to a kind of populism, cut off from technical, legal and geopolitical realities and completely eliminating from the equation the criterion of "place of storage of the data".

15. The location of the data does matter.

As a very good panel of *computer* and *data scientists* in an *Amicus Curiae* filed in the Court of Appeal has shown[14] the place of storage is of great technical importance: the data has a "physical location" and is stored using hard drives in *data centre*s located in specific countries. When accessing emails, this technically means that data are retrieved from a specific physical space where they are stored. The data therefore has a much greater "materiality" than is often suggested. Companies like Microsoft have invested hundreds of millions of euros to build *data centres* in some *specific places* on the basis of both performance considerations (mainly related to geographical proximity between the user and the storage location) and *legal ones* linked to *data protection*. So, especially since the revelations of E. Snowden, companies like Microsoft have created several data centres in Europe (Germany, France, Ireland, The Netherlands, The United Kingdom) and have decided to store European data in Europe[15] - to give them the assurance that they would be covered by European data protection law (including the GDPR) and would not be accessible to the US authorities without going through the formal procedures provided by international law. So, far from being "fortuitous", the place of storage in the *Microsoft Ireland* case is very important technically and legally and to circumvent it by claiming that "there is no extraterritoriality" in the US mandate would lead to serious consequences.

16. Ireland thinks there is extraterritoriality.

Another indicator of the existence of an element of "extraterritoriality" in this case is the reaction of Ireland, the place where the Microsoft *data centre* is located. The Judge who had ruled in favour of the US government (and whose decision was overturned by the Court of Appeal) had claimed that there was no extraterritorial effect because the warrant "*does not criminalize conduct taking place in a foreign country" and "does not involve the deployment of American law enforcement personnel abroad"*.[16] In short, access by the US authorities to emails stored in Ireland would in no way affect Ireland, so there would be no extraterritoriality. The problem, however, is that Ireland does not seem to share this analysis. In an Amicus curiae submitted to the US Court of Appeals, Ireland points out that it has"a genuine and legitimate interest in potential infringements by other States of its sovereign rights with respect to its jurisdiction over its territory", while indicating that it would be ready to consider "as expeditiously as possible" a request for mutual legal assistance, if the United States made such a request under the Mutual Legal assistance Agreement (Mutual Legal assistance Treaty - "MLAT") between the two countries.[17] Even if Ireland is not actually accusing the United States of a violation of its sovereignty (which can be understood in the light of the friendly relations between the two countries), its *Amicus curiae* is a clear indication of the extraterritorial nature of the case, which should, in principle, be settled through international law.

17. The European Union thinks there is extraterritoriality.

Apart from Ireland itself, it is also necessary to consider the whole mosaic. For several years now, the European Union has developed a very protective legal regime for personal data and privacy. The effective entry into force of the General Data Protection Regulation (GDPR) in May 2018; the transposition at the same time of Directive 2016/680 on the *protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data* ; the current negotiation of the *ePrivacy* regulation on respect for privacy and the protection of personal data in electronic communications; the conclusion of several international agreements (including the *Privacy Shield*); and many other activities testify to the will of the European Union not only to put in place strong protection of personal data and private life in Europe, but also to ensure that the data of European citizens and residents stored in Europe may only be transferred abroad (including to third-country authorities in the framework of an investigation procedure) under certain strict conditions, including compliance with specific procedures and the existence of sufficient guarantees. In this framework, it is not surprising that, for the European Union, the mandate given to Microsoft by the US authorities is considered "extraterritorial" and could even be perceived as an attempt to circumvent the legal protection put in place in Europe. The European position in this regard was very well summed up in a 2014 statement by Viviane Reding, then Vice-President of the European

Commission and Commissioner for Justice, Fundamental Rights and Citizenship, who reacted to the decision of the US court of first instance (which found for the US government) as follows:

"The effect of the US District Court order is that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign government requests for access to information and ensure certain safeguards in terms of data protection. The Commission's concern is that the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union. […] The Commission has raised this issue with the US government on a number of occasions. The Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers".[18]

Even more explicitly, the Vice-Chairman of the LIBE (Civil Liberties, Justice and Home Affairs) Committee of the European Parliament, Jan Philipp Albrecht, pointed out in an Amicus Curiae submitted to the American Court of Appeal that:

"Personal data located in EU territory is subject to strict rules designed to maintain the autonomy of the affected individual (data subject). Those rules apply to the email account covered by the warrant in issue in this case. They balance the protection of the individual's rights with the necessity of data processing for public interests, such as law enforcement. […] The decision of the District Court effectively permits this carefully constructed regime to be sidestepped. […] It is fair to record that there are major differences between the U.S. and European laws on data protection. The European standard is much more severe than the U.S. standard. […] For U.S. law to treat data stored in Europe as if it were stored in the United States is a territorial encroachment without justification, and one which is exacerbated by the sharp differences in the legal status of personal data in the U.S. and the EU. […] This unilateral exercise of jurisdiction over data held in the EU puts into serious jeopardy the level of trust between the EU and U.S. on data protection matters".[19]

In the light of all these factors brought to its attention, one can understand why the US Court of Appeals took a decision in favour of Microsoft, considering that there was an "extraterritorial and illegal application of the law" and severely criticising "the theory that no infringement is made on the interests of the foreign sovereign State when a US judge orders a service provider to "collect" from servers located abroad and "import" to the United States data that may belong to a foreign national [...]".[20]

Since the US Court of Appeals decision and ahead of the US Supreme Court judgment, similar strong statements have been made in Europe by highly qualified authorities, such as the Article 29 Working Party, uniting all EU Data Protection Authorities ("DPAs"), which, discussing the Microsoft Ireland case concluded in an opinion issued the 29 November 2017 that:

"EU data protection law provides that existing international agreements such as a mutual assistance treaty (MLAT), must – as a general rule - be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers. The circumvention of existing MLATs or other applicable legal basis under EU law by a third country's law enforcement authority ***is therefore an interference with the territorial sovereignty of an EU member State.*** *Vice versa, EU law enforcement authorities should also - as a general rule - be required to respect existing international agreements such as MLATs or any other applicable legal basis under EU law when requesting access or disclosure from data controllers in third countries".*[21]

18. The behaviour of the United States seems to indicate that extraterritoriality is present.

Going even further, one might ask whether the American behaviour itself could not give some clue to the existence of an extraterritorial situation in any case of transfer of data stored in Europe to the United States. In this regard, it should be emphasised that States have, in recent years, increased the conclusion of mutual legal assistance agreements ("MLAT", cf. §6, 16, 22 and 30) in order, above all, to cope with the new challenges of cross-border cooperation and access to digital evidence in the digital age. Thus, according to a study conducted between 1977 and 2013, the number of MLATs grew from a few to several hundred.[22] The United States has concluded MLATs with more than 60 countries - including a number of European countries, notably Ireland and France. The United States has also concluded a MLAT (entered into force in 2010) with the European Union itself, one of the objectives (Article 9) of which is to take into account the requirements for the protection of personal data within the European Union.[23] In concluding this agreement, **the United States recognised that US courts "lack the authority to subpoena evidence in a foreign country"**[24], which seems to run counter to the US government's current case before the Supreme Court. They also recognised that, in principle, the production of evidence located in a European country implies an element of extraterritoriality and should be conducted through channels of mutual legal assistance.[25] Apart from the MLATs, the United States has also concluded in recent years a series of agreements (Privacy Shield, PNR, agreement on the transfer of financial messaging data, etc.) which are *all* based on the idea that not only is there *transfer of* data stored in Europe to the United States (and therefore clearly *extraterritoriality*), but, moreover, that this transfer can only be performed in compliance with the *protection* granted to European data.

19. Conclusion.

The above elements clearly show that the argument that "there is no extraterritoriality" in the US government's injunction for ISPs to transfer data from Europe to the United States cannot be accepted. This should be enough for the US Supreme Court to uphold the decision of the Court of Appeal in favour of Microsoft. Nevertheless, it is necessary to reflect on the consequences that a decision of the Supreme Court in favour of the American government might have.

III. The possible consequences of a judgement in favour of the American government

20. Cassandra's curse.

It is always difficult and risky to predict the future - especially in cyberspace. However, it is legitimate to have some concerns about the negative consequences that a Supreme Court ruling in favour of the US government could have. Not necessarily all of these consequences will be realised, some being exclusive of others. Their occurrence will depend on the behaviour of the various players involved - which is not always easy to predict. It is, for example, difficult to predict whether the European countries and the European Union will tenaciously react to such a judgement of the Supreme Court - or whether they will prefer to keep a "low profile" on the grounds that, by circuitous and impenetrable paths, such a judgement could also have some positive effects. Some officers in EU countries might, for example, hope such a judgement to have the potential to facilitate their own access to digital evidence if only the United States were "generous" with its European allies - even though such "generosity" would be not only uncertain (as there will be no obligation to do so) but also, by definition, legally restricted.[26] Some European governments could also hope that such a Supreme Court ruling would have the miraculous effect of promoting the emergence of a European cloud industry. We will, however, make some brief remarks about the consequences that seem particularly plausible given the parameters of the case.

21. A dangerous risk of imitation?

It is to be feared that, if the Supreme Court accepts the argument of the American government and the criterion of "where the data is accessible", each country could be tempted to do exactly the same. If we consider that an operation consisting of asking an Internet provider to "transfer" the emails of a foreigner stored abroad does not include "any element of extraterritoriality", then all countries could formulate similar requests subject only to the proviso that: a) the ISP has an office in the territory of the requesting country (Microsoft, for example, has subsidiaries in more than 120 States); and b) that there is a mandate (or even a simple proceeding) against a person suspected of violating national law. From the point of view of the protection of human rights, the mere prospect that this procedure could be used against journalists accused by foreign governments of undermining "national security" by their investigations or writings, or against persons accused of "blasphemy" for their position on religious questions, is enough to illustrate the extent of the problem. From the point of view of inter-state relations, the fact that States are circumventing international cooperation mechanisms in order to "help themselves" to data stored in other countries could cause very strong tensions and profoundly destabilize international law. Is the United States willing to allow foreign countries to instruct local GAFAM (and other) affiliates to let them collect unilaterally, and without asking the

US authorities, data from US citizens stored in the United States but "accessible by a single click" from their respective capitals? "*We would go crazy if China did this to us*" pointed out Microsoft's attorney before the Court of Appeal. Or is the United States hoping that the model they are trying to promote in the Supreme Court will only benefit them and will only be applicable to the "headquarters" country - but not to the affiliates' countries? Such a hope seems rather futile. The model of "unilaterally helping ourselves in the territory of other countries" will undoubtedly be followed by others, if only on the basis of the principle of reciprocity, and could start a dark episode for peaceful coexistence and international cooperation based on the law.

22. A weakening of international mutual legal assistance agreements?

Apart from the tensions that could arise between the States, such unilateralism in data collection could affect the functioning of specific international agreements and especially the MLATs concluded between the United States and third countries. If the United States embarks on a unilateral collection of "digital evidence" no matter where it is stored, this would mean that it would no longer need to use MLATs (or other international cooperation mechanisms) to obtain such data. This would therefore mean: either **1)** that the MLATs will undergo a profound imbalance - third countries being still required to ask the US authorities, through the MLATs, for data stored in the United States while the United States no longer needs these countries to access data stored in the territory of the latter; or **2)**, if all countries follow the US unilateralist model, the MLATs will become obsolete in their "digital evidence" dimension.

23. A weakening of the protection of privacy and human rights?

If the previous observations concern interstate relations, it is also necessary to integrate *the individual* dimension into the problem. What would be the effect of a decision of the Supreme Court favourable to the US government? What would happen if other countries were inspired by such case law into requiring subsidiaries of ISPs to submit personal data to them in other jurisdictions? Such a situation could seriously affect data protection and privacy. The protections developed in Europe by a dense network of instruments to protect personal data against possible abuses by the authorities in the post-Snowden world could be circumvented by foreign countries determined to unilaterally access personal data produced and stored in Europe, without the requirement that the authorities of European countries had to be consulted within the framework of the traditional mechanisms of international law. Other rights could also be affected, such as freedom of expression and freedom of the press (see the examples mentioned above in § 21), including the protection of press sources, or even legal privilege between lawyers and their clients. In addition, the right to an effective remedy could be seriously weakened. A French national knows, for example, that the

French State can access his emails and other documents stored in servers in France, if he is the subject of a judicial inquiry, or that France could transmit his personal data to a foreign country in the framework of a MLAT or a legal assistance request. But he also knows that, if the authorities act abusively (by, for example, bypassing the framework of the French and European Convention of Human Rights Law or the principles of necessity and proportionality), he can appeal to the French courts and that, if the French courts fail to protect him, he can appeal to the European Court of Human Rights (ECtHR). If, on the other hand, the United States unilaterally accesses his data, the French national (even assuming that he is aware of it - which is far from guaranteed) will not be able to appeal against his country because it is not involved in the transmission of data. It will not be able to approach the American courts either, because, quite apart from the impracticability of such a move, foreigners resident abroad are not protected by the Fourth Amendment, which provides "The right of the people to be secure […] against unreasonable searches and seizures". The only possible remedy will therefore be to take action against the internet and cloud provider, which will then be in a situation of almost inextricable conflict of laws.

24. Conflicts of laws.

Imagine that the Supreme Court rules in this case against Microsoft and that the company is tomorrow, in a similar case, forced to provide the US authorities with the personal data of a French national and resident stored in France. To the extent that this transfer is performed by Microsoft, it will constitute a violation of both French law and European law. Admittedly, both French law and European law allow the transfer of personal data to foreign authorities, but only on the condition that this is done within a framework recognised by international, European or national law (with "national" meaning the law of the country where the data is located). To understand the legal regime in this area, it is necessary to refer to article 48 of the GDPR, which reads as follows:

"Article 48. **Transfers or disclosures not authorised by Union law** Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data ***may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty,*** in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter". (emphasis added)

In its cert petition to the Supreme Court,[27] the US government argued that if Microsoft transferred the personal data to the United States on the basis of the SCA warrant, there would be no violation of the GDPR. According to it, the last phrase of Article 48 ("without prejudice to other grounds for transfer pursuant to this chapter") shows that there are exceptions, especially that of Article 49 (§1d) of the GDPR which provides

for a derogation from Article 48 if "the transfer is necessary for important reasons of public interest". The American argument therefore seems to be that, to the extent that the data transfer warrant has been issued in the framework of a judicial inquiry, "the transfer is necessary for important reasons of public interest". It seems to us that this is a misreading of the GDPR. The derogation for "important reasons of public interest" in Article 49 does not refer in any way to the assessment of what constitutes such a ground for a foreign country. Such a reading would be absurd, because any country could then argue the existence of an "important ground of public interest" to get their hands on the personal data of Europeans. The derogation in question actually refers to the law in force *in the European Union*. It means that a transfer of personal data to a third country "without a valid EU legal basis" lead to "a breach of EU data protection law".[28] The GDPR itself unambiguously explains this point in its recital 115.[29] The argument of the US government cannot be accepted. The conclusion is that if Microsoft obeyed and implemented the US warrant to submit data from a European stored in Europe without going through the legal channels provided by the GDPR, Microsoft would be breaching both the GDPR and the national legislation of the country concerned. This would expose it to civil and criminal prosecution and the risk of an administrative fine which, for this reason, could amount, according to Article 83§5 of the GDPR, to EUR 20,000,000 or to 4% of the total worldwide annual turnover of the preceding financial year. A decision of the Supreme Court in favour of the US government would expose not only Microsoft, but also *all* ISPs located in both the United States and Europe to inextricable conflicts of laws. Unless the ISPs can find ways to deprive the decision of the Supreme Court of effect – an issue to which we will now turn.

25. Balkanisation of the internet?

Considering that it is preferable to avoid fines of up to 4% of global turnover by European Data Protection Authorities (or to be subject to similar fines in the United States), the ISPs could adopt strategies to circumvent the decision of the Supreme Court. As explained above the Supreme Court will only be able to adopt a decision in favour of the government if it accepts the argument of the latter that only the place from which the data is accessible is relevant. However, to avoid the applicability of this criterion, it will be sufficient to develop technical solutions so that the data is no longer accessible by the ISP outside the country where it is stored. This is already being done, in advance, in some countries. In Germany,

Microsoft has devised a "data trustee" mechanism, based on commercial agreements that grant a third party responsibility for its *data centres* to protect itself against any legal proceedings from outside. Microsoft has opened *data centres* in Frankfurt and Magdeburg and then entrusted T-Systems with the task of being the data keeper and controlling all access to the data stored there. So legally, Microsoft "does not have access" to these data from the United States because only T-Systems has the legal authority to disclose the data that is stored in these *data centres*.[30] IBM has recently taken up this idea, devising a different configuration but one that leads to the same result: what is done in Germany (in terms of data) remains in Germany - and its cloud is not accessible to IBM personnel outside Europe.[31] Other ISPs are now considering encrypting data in *data centres* so as to entrust the keys to the clients, who would be the only persons able to decrypt their personal data and access it. There is no shortage of technical solutions to deprive the criterion of "the place where the data is accessible" of any meaning. One may therefore wonder what would be the point of a decision of the Supreme Court favourable to the government. Ultimately, it could be counterproductive for LEAs, by encouraging, in particular, widespread encryption of data in the cloud, which could frustrate the activities of law enforcement agencies. Such a US Supreme Court decision could also feed into an extreme movement of cyber-protectionism and "data localisation", well explained in the Chertoff's Group study[32], characterised by "nationalisation" not only of data storage but also of storage providers. The "balkanisation" movement of the Internet that could ensue from this would, in fact, be in nobody's interest: neither the public authorities, which could have much greater difficulty than today in accessing the "evidence in the cloud"; nor cloud or Internet players, whose business model could be affected; nor individuals, for whom the unbridled proliferation of "digital great walls" would undermine what is so much the strength of the internet.

26. Conclusion

A "victory" of the government in the legal battle against Microsoft in the Supreme Court could only be a "Pyrrhic victory". *Everybody* would end up losing, including the United States and its technology companies. Rather than persist in a risky and unilateral approach, the United States and all States should engage in the search for *multilateral* solutions to these transnational problems, solutions that are the only ones capable of cutting the Gordian knot of access to evidence in the clouds.

IV. Possible solutions

27. In search of a new legal regime.

If the Supreme Court, on the basis of the considerations presented in Part II of this study, rejected the request of the American Government, this would avoid some among the negative consequences mentioned in Part III. But such a rejection would not solve the difficulties that police and law enforcement services face in accessing digital data and evidence (§7). Solutions compatible with international law and the protection of human rights must therefore be sought to enable law enforcement and justice to perform their functions. The big question is what this legal regime might be. The answer to this question is particularly complex and goes well beyond the scope of this study. We would, however, like to put forward some ideas to show that there are indeed alternatives to the unilateral solutions advocated by the US government in the Supreme Court. We will begin with a global reflection on the criteria which should be taken into account to build the substance of this legal regime (§28), before devoting some reflections (§29-32) to *mechanisms and proceedings* which could be operated.

28. On which criteria should this legal regime be constructed?

It is imperative for States to carry out an in-depth study of the *types of data* and the criteria on which a coherent legal regime could be built. First, we believe that such a legal regime should differentiate according to data types sought during criminal investigations. The problem, as we have seen (§4), does not arise in the same way for "subscriber information" and "content data" - and it is imperative to also include "traffic data" (or "metadata") in the equation. Secondly, it seems quite obvious that neither the criterion advocated by Microsoft before the Supreme Court (that of the "*place of storage of the data*" or - still less - the criterion of "*place of accessibility of the data*") advocated by the US government are sufficient to build a satisfactory legal regime. Other criteria should enter the equation, which would put the individual at centre stage. So, *the nationality of the data owner and the place where the data owner resides/is located* should be important criteria in the construction of this legal regime. It is true that these criteria could be difficult to establish at the start of a criminal investigation - to the extent that criminals could use spoofing and "hide" their identity, IP address or the place from which they operate. But very often this is not the case, and these criteria could play their full role. Other criteria might also include the ISP headquarters; the location of the ISP subsidiaries; the country where a cloud service provider offers its services; the scale of the service provider's activity in that country; or the law of the State in which the suspect has subscribed to a service.[33] In any case, the legal regime built on types of data and

these criteria should introduce "checks and balances" to avoid abuses and to address the protection of human rights, due process concerns, transparency, independent oversight and accountability.

29. National laws to solve problems of international law?

Let us therefore turn now to the process which could support such solutions. One could, first of all, question the desirability of solutions introduced exclusively by national laws. From an operational point of view, States may wish to promote this path as it is faster than the mechanisms of international law and allows them to preserve their autonomy. The problem, however, is "that it takes two to tango". Unilaterally adopting laws that affect the jurisdiction and sovereignty of other countries will not solve virtually any of the issues raised in Part III of this study. During the proceedings before the American courts, there were extensive discussions of the recent submission to the American Congress of the "ICPA" bill (§8). Even Microsoft suggested that this law "would solve the problems." However, it is permissible to hold a more nuanced opinion. Without being able to proceed here to an analysis of this legislative proposal, which is at the very early stage of its consideration by Congress and whose adoption process could take years, it is enough to note its main characteristics. The ambition of the ICPA is to fill the gaps in the SCA by clearly giving extraterritorial scope to a warrant similar to that issued in the *Microsoft Ireland* case. The ICPA tries, however, to mitigate the risk of undermining the sovereignty of States (or, more precisely of some States which are to be included in a list attached to this law) where the data are stored, on the expectation that the obligation for ISPs to provide data to the US administration would only be required if the authorities of the country in question received a notification for this purpose and did not object to the transfer of the data (usually within 14 days). This is, therefore, legally a matter of international implied consent introduced unilaterally by the United States. The law provides, moreover, for derogations from this procedure, including if an American judge "determines that the interests of the United States in obtaining the information outweigh the interests of the qualifying foreign government in preventing the disclosure". Even though this ICPA is an evolution from what the government is requesting from the Supreme Court, it is likely to create some of the problems mentioned in part III. This shows the limits of a solution reached through the sole adoption of national laws: the United States cannot impose its law - or the implied consent procedures it contains - on other nations, while reserving the right not to not respect the will of other nations whenever the US Judge considers it necessary. These kinds of things can only be done through the mechanisms of international law: negotiation and consultation

between countries and the conclusion (in a more or less formal manner) of *international agreements* to solve problems. The procedures of *implicit consent* provided by the ICPA could only be effective internationally or avoid conflict of laws if they were *accepted* by other countries and if they included an element of *reciprocity*. International law thus seems unavoidable. Three solutions (which could indeed be combined) might therefore be considered.

30. An improvement of the MLATs?

In a detailed report on the issue, the Council of Europe's "Cloud Evidence Group" concludes that "mutual legal assistance remains the main means of obtaining electronic evidence from foreign jurisdictions for use in domestic criminal proceedings".[34] One way to strengthen mutual legal assistance would be to improve bilateral mutual legal assistance treaties, the so-called MLATs (§6, 18 and 22). These treaties are often accused of being inefficient in obtaining electronic evidence. According to a study by the Committee on the Convention on Cybercrime (T-CY)[35], response times to a request for such evidence can range from six to 24 months.[36] "Many requests and thus investigations are abandoned" as a result and this "adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence".[37] The Committee adopted a series of recommendations aimed at making the process more efficient. Academic studies have also made important suggestions for its improvement. However, several observers point to the limitations of the MLAT system. The number of requests for mutual legal assistance to access data is increasing dramatically from year to year. As the T-CY Working Group asks: *"Is it realistic that the number of MLA requests sent, received and processed can be increased by a factor of hundred or thousand or ten thousand? Are governments able to dramatically increase the resources available for the efficient processing of mutual legal assistance requests not only at the level of competent central authorities but also at the level of local courts, prosecution and police offices where MLA requests are prepared and executed?"*[38] Moreover, if the solution were to come only from bilateral mutual legal assistance agreements, it would be necessary to have 18,528 MLATs to treat the problem at the level of the 193 countries of the UN![39] It is obvious that MLATs are not a panacea.

31. The invention of a new type of agreement: from MLATs to DSAs?

A second solution, which could be combined with the first, could be to introduce a new type of agreement: "Data Sharing Agreements" (DSAs), whose sole objective would be to facilitate the access of law enforcement services to communications and digital evidence - while providing

sufficient substantive and procedural safeguards for human rights. Last year, there were media reports that the United States was negotiating such an agreement with the United Kingdom.[40] Little information has been leaked about the content of this agreement, but it appears that it may allow the UK authorities to require ISPs located in the United States to provide personal data that is the subject of a criminal investigation. However, such a request could only concern third-country nationals - and not the data of a US national or permanent resident for whom the United Kingdom would still have to go through the MLAT, requesting such data from the US authorities themselves. On the other hand, it is not known whether this DSA agreement is subject to a condition of reciprocity (with the same guarantees for British nationals). In any case, and whatever at the moment the questions that this draft agreement raises[41], including human rights safeguards, it is likely that this precedent will be carefully monitored by the international community and that other countries could engage in the negotiation of such DSAs. The problem, however, is that the bilateral track is also limited here. The same mathematical rule as for the MLATs applies, requiring the conclusion of 18,528 DSAs to address the problem at the level of the 193 UN countries (unless one assumes that only the DSAs with the United States would have a practical interest). It is therefore necessary to find faster solutions to implement effective DSAs. In this respect, the European Union is currently working on a new legislative package entitled "e-evidence", which is intended, precisely, to facilitate access to digital evidence between the countries of the EU.[42] One could imagine that if this project were to succeed the next step could be the conclusion of a DSA between the United States and the EU - a DSA which should include human rights and due process guarantees[43] as well as "equivalent protection" provisions and mechanisms of verification and accountability.

32. A Protocol to the Budapest Convention?

Last but not least, States could consider resolving these issues by concluding a single multilateral international convention. Since the problem is urgent and concerns *all States*, the negotiation of a universal convention on access to digital evidence seems to be a logical solution: no need to conclude 18,528 agreements, only one is enough! But the conclusion of such a universal agreement seems, for the time being, to be totally unrealistic. The differences, controversies and mistrust surrounding cyber/data issues loom so large between States that the conclusion of such an international agreement seems impossible. On the other hand, it is much more realistic to move forward quickly in some multilateral frameworks, where very significant progress has already been made by States. More specifically, we are thinking of the countries which are party to the 2001 Budapest Convention on Cybercrime. This convention is already binding on 56 countries, including the United States and a very large

number of EU and Council of Europe countries. It is, moreover, taking on a new dimension with its gradual acceptance not only by some countries of Latin America and Africa but also Israel and Japan. The Committee established by this Convention has recently set up a Group which bears, perhaps, the most mysterious name of all international institutions: "Cloud Evidence Group".[44] This Group has conducted interesting work on the issue and is at the centre of the initiative announced in June 2017[45] by the Council of Europe concerning the conclusion of a protocol to the Budapest Convention on Evidence in the Cloud, which could resolve many of the difficulties mentioned in our study and which should fully take into account human rights and due process issues while providing for transparency, oversight and accountability. Negotiations for the conclusion of this protocol are expected to last "at least two and a half years" - but nothing prevents States from speeding up the process to address urgent needs reported by their law enforcement and police services.

33. Conclusion.

International law offers States various possibilities to find mutually acceptable, sovereign-respectful solutions, compatible with the protection of human rights, to the important problem of access to digital evidence for criminal investigations. States have the choice between the rather risky unilateralism advocated by the US government in the US Supreme Court and the multilateral path that has proven its effectiveness time and again in the history of international law.

Références

[1] *For example, the Parties to the Budapest Convention submitted 227,962 requests in 2015 to leading US service providers (Apple, Facebook, Google, Microsoft, Twitter and Yahoo) and obtained (at least partial) data in about 67% of cases. The overwhelming majority of requests and especially disclosures relate to "subscriber data". See Final Report of the "Cloud Evidence Working Group" of the Council of Europe Convention on Cybercrime Committee, T-CY (2016) 5, 16 September 2016, p. 30.*

[2] *By an injunction of 24 January 2013, the District Court of Paris ordered Twitter to provide identification data of the authors of racist or anti-Semitic messages. While Twitter had argued that it could not do so because the information in question "was stored in the United States," the Court insisted that Twitter had an obligation to submit it because it was only data relating to subscribers, who were French residents in France, subject to French law under French legislation and Twitter's own terms and conditions of use. In a communication to the Council of Europe France clarified that, whereas it considered that it had a title to request technical/declarative data, "**requests for content are only possible through international judicial cooperation**". See Cybercrime Convention Committee (T-CY) Cloud Evidence Group, Application of Article 18.1.b Budapest Convention on "production orders": Compilation of replies to the questionnaire, 18 February 2016, T-CY (2015)22), p. 15.*

[3] https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/08/Second-Circuit-Concurring-Opinion.pdf , p. 15.

[4] In such a case, for example, could it be possible to construct a legal presumption according to which the data are held in the country where the crime has been committed?

[5] Cf. US District Court Affidavits of Michael McDowell, former Attorney General, Minister of Justice and Deputy Prime Minister of Ireland, 5 June and 23 July 2014 (declaring that: "Some [MLAT] requests, such as a request for a deposition, can take months from start to finish. Other requests, such as requests for digital evidence, are generally fulfilled within a matter of weeks. […] If necessary, urgent requests can be processed in a matter of days". (emphasis added). See https://www.supremecourt.gov/DocketPDF/17/17-2/22918/20171206204555098_United%20States%20v.%20Microsoft%20Joint%20Appendix.pdf, at 122.

[6] U.S. Government reply to Microsoft's brief in opposition of cert, at 4.

[7] https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/08/Second-Circuit-Majority-Opinion.pdf at 42.

[8] https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/08/Second-Circuit-Concurring-Opinion.pdf at 1.

[9] https://www.congress.gov/115/bills/s1671/BILLS-115s1671is.pdf

[10] U.S. Government reply to Microsoft's brief in opposition of cert, at 4.

[11] Ibid., at 1-2.

[12] T. Christakis, "Necessity Knows No Law"? "General Report on Necessity in International Law", in Necessity in international law, colloquium of the French Society for International Law, Paris, Pedone, 2007, pp. 9-62.

[13] Brigitte Stern, quoted in Jean Salmon (ed.), Dictionary of Public International Law, Bruylant, 2001, p. 211. Cf. also M. Kamminga, "Extraterritoriality", MPEPIL: "The terms 'extraterritoriality' and 'extraterritorial jurisdiction' refer to the competence of a State to make, apply and enforce rules of conduct in respect of persons, property or events beyond its territory. Such competence may be exercised by way of prescription , adjudication or enforcement".

[14] Amicus brief from computer and data science experts

[15] See for example:
https://blogs.office.com/en-us/2017/10/27/delivering-a-faster-and-more-responsive-outlook-com/?eu=true which specifies that: "if you are in Europe when setting up your account, your email will be stored in Europe". For «business» data see https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located

[16] https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/02/Magistrate-Judge.pdf at 21.

[17] Amicus brief from the Republic of Ireland, at 1 and 4.

[18] Letter by Viviane Reding, then Vice President of the European Commission Justice, Fundamental Rights and Citizenship, 24 June 2014 https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/02/Scan-Ares-MEP-int-Veld-.pdf

[19] *Amicus brief from MEP Jan Phillip Albrecht, pp.7-8.*

[20] *https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/08/Second-Circuit-Majority-Opinion.pdf, at 42.*

[21] *Statement of the ART 29 WP on e-Evidence, 29 November 2017, at 9. (emphasis added).*

[22] *Sarah Cortes, "MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance", 22 Rich. J.L. & Tech. 1, 26 (2015)*

[23] *See https://www.state.gov/documents/organization/180815.pdf*

[24] *https://www.congress.gov/110/crpt/erpt13/CRPT-110erpt13.pdf. at 2 (emphasis added).*

[25] *According to the United States: "[MLATS] generally address the production of records located in the requested State". Quoted in https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/12/DigitalRightsIreland-AmiciBrief.pdf, at 16.*

[26] *In any case, the "generosity" in question could not concern content data located on American soil because the SCA law is an obstacle to that. The Europeans could not hope to access it without going through the procedures of the MLATs with the United States. So there will be no "reciprocity" in this area and we will slide towards a legal asymmetry in transatlantic relations.*

[27] *Supra, note 6, at 8.*

[28] *As the Article 29 Working Party on Data Protection had already pointed out in its Opinion of 05/2012 on Cloud Computing (adopted on 1 July 2012)., at 5. See also note 21.*

[29] *"Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject" (emphasis added).*

[30] *See https://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/ and https://www.meritalk.com/articles/u-s-cant-touch-microsofts-overseas-data-centers/*

[31] *See http://www.datacenterknowledge.com/regulation/ibm-cloud-hands-german-users-control-their-data as well as http://www.zdnet.com/article/cloud-computing-ibm-overhauls-data-access-rules-at-euro-data-centre/*

[32] *As the Chertoff Group points out: "trends toward data localization will almost certainly accelerate, likely to the point of what one could term "extremely restrictive data localization" (at 4).*

[33] *For a discussion of all these criteria, see the Final Report of the "Cloud Evidence Working Group" of the Council of Europe Convention on Cybercrime Committee, T-CY (2016) 5 , September 16, 2016.*

[34] *Ibid., at 35.*

[35] *https://rm.coe.int/16802e726d at 45.*

[36] *However this is an average of all kind of MLATs requests. See for example supra note 4 the affidavit of the former Attorney General and Minister of Justice of Ireland assuring that, within the context of the US/Ireland MLAT, "requests for digital evidence, are generally fulfilled within a matter of weeks" and "If necessary, urgent requests can be processed in a matter of days".*

[37] *Final Report of the Evidence in the Cloud Task Force, supra note 33, at 11.*

[38] *Ibid, at 10.*

[39] *The calculation is ours, but for the idea see P. Swire, J. D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program", 71 N.Y.U. Ann.Surv. Am. The. 687, 738 (2016).*

[40] *https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html*

[41] *For an American point of view see https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/*

[42] *Cf. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en*

[43] *In its latest Report on Combating Cybercrime, published on 25 July 2017, the LIBE Committee of the European Parliament stresses: «Stresses the need for any e-evidence framework to include sufficient safeguards for the rights and freedoms of all concerned; highlights that this should include a requirement that requests for e-evidence be directed in the first instance to the controllers or owners of the data, in order to ensure respect for their rights, as well as the rights of those to whom the data relates (for example their entitlement to assert legal privilege and to seek legal redress in the case of disproportionate or otherwise unlawful access); also highlights the need to ensure that any legal framework protects providers and all other parties from requests that could create conflicts of law or otherwise impinge on the sovereignty of other States».*
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bREPORT%2bA8-2017-0272%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN , §65.

[44] *https://www.coe.int/fr/web/cybercrime/ceg*

[45] *https://www.coe.int/fr/web/human-rights-rule-of-law/-/cybercrime-towards-a-protocol-on-evidence-in-the-clo-1?desktop=false*

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused on security and risk management. Founded in 2009, The Chertoff Group helps clients grow and secure their enterprise through business strategy, mergers and acquisitions, and risk management security services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group maintains offices in Menlo Park, California, and New York City, New York. For more information about The Chertoff Group, visit www.chertoffgroup.com.

ABOUT CEIS

Founded in 1997, CEIS is a strategy and risk management consulting company working primarily for French and European institutions and strategic sectors.

CEIS' missions include security, economic intelligence (ethical and financial compliance, anti-fraud, pre-litigation, competitive risks ...) and digital security, both on strategic and operational levels. CEIS conducts prospective studies and consultancy missions in cybersecurity and digital transformation, and has developed a strong operational Cyber Threat Intelligence team.

In 2017, CEIS co-founded BlueCyForce, the first European training center dedicated to cyber defense (www.bluecyforce.com), with the company Diateam.

Since 2013, CEIS co-organizes the International Cybersecurity Forum (FIC) (www.forum-fic.com) and manages numerous observatories on digital security such as the FIC Observatory or the Cybernetic World Observatory on behalf of the Ministry of the Armed Forces.

Headquartered in Paris, CEIS also has a European office in Brussels. It employs 80 consultants and around 20 associate experts. For more information, visit www.ceis.eu

THEODORE CHRISTAKIS

Theodore Christakis is a Professor of international law at the University Grenoble Alpes and a Senior Member of the Institut Universitaire de France (IUF). Since 2005, he also holds a teaching appointment at the Paris School of International Affairs (Sciences-Po Paris). He is Director of the Center for International Security and European Studies (CESICE) and Deputy Director of the Grenoble Alpes Data Institute.

He is founder and co-chairman of the European Society for International Law's *Interest Group on Peace and Security*, a member of the International Law Association's *International Committee on Use of Force*, a member of the editorial board of the *Leiden Journal of International Law* (Cambridge University Press) and the Scientific Board of the *Revue Belge de droit international* and the *Australian Yearbook of International Law* He was also a member of the Executive Council and the Board of the *French Society for International Law* (SFDI) for 12 years.

Over the recent years he was visiting professor in several foreign institutions and was invited more than 70 times to present his work in several conferences, workshops and seminars held in 27 countries. He has published 9 books and is the author or co-author of more than 60 scientific articles and chapters. His recent publications include the book *Cyber-Attacks. Prevention-Reaction: The Role of States and Private Actors*" (with K. Bannelier, Revue Défense Nationale, Paris, 2017) which was the preliminary study to the International Conference *Building International Peace and Security in Cyberspace* organized by the French Government in UNESCO on 6 and 7 April 2017. (https://ssrn.com/abstract=2941988)

Theodore Christakis has regularly served as Legal Counsel for Governments, International Organisations and Business in issues concerning International Law, Cybersecurity and Data Protection, including the implementation of the EU General Data Protection Regulation (GDPR). He intervenes as external consultant for CEIS.

NOTES

DECEMBER 2017