II.2

Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?

SUMMARY: 1. The argument and background of the paper. – 2. An overview of the *U.S. v. Microsoft* litigation and the U.S. Cloud Act. – 3. Possible motivations for a *comity-upon-request* rule and the "information problem". – 4. Assumptions and observations supporting the "information problem" view. – 5. Clashing state interests: Securitization of private data flows and the facilitation of global market access. – 6. Data location as a connecting factor. – 7. The proxy theory of connecting factors. – 8. Conclusion.

1. This paper focuses on a new framework provided by the U.S. "Clarifying Lawful Overseas Use of Data Act" (hereinafter "Cloud Act")[336] that is designed overcome jurisdictional conflicts with regards to law enforcement orders compelling service providers to disclose user data that is stored abroad on cloud computing based systems.

The Cloud Act was passed by the Congress in March 2018, bundled in a yearly budget act and passed without much discussion in the legislature. The Cloud Act seeks to circumvent the jurisdictional problem by authorizing disclosure warrants compelling service providers resident in the U.S. to disclose user information to U.S. authorities wherever the information is stored, but at the same time allowing the service provider to move to quash the compelling order ("warrant") in cases where the service provider finds it on its own initiative and discretion that the compliance with the order risks giving rise to a conflict of laws. The law sets guidelines for a "comity" assessment that the court will undertake upon a motion to quash duly made by the service provider. I argue that a motivation on the part of the U.S. government to create such a solution may be an interest in facilitating global market access of U.S. service providers without forfeiting more of its prescriptive authority than necessary. I further argue that this motivation should be studied as a universal central trend that is shaping the global regulation of data flows.

336 *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, H.R. 4943, enacted by *Consolidated Appropriations Act, 2018*, Pub. L. 115-141, 23 March 2018 (https://www.gpo.gov/fdsys/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm).

2. The Cloud Act became law just in time to render the *U.S.* v. *Microsoft* [337] (hereinafter "*Microsoft*") case before the U.S. Supreme Court moot, dodging (at least for a time) international repercussions that would result from a generally applicable Supreme Court judgment. That case concerned the refusal of Microsoft Corporation to disclose to the FBI user data that was stored in a data center located in Ireland upon the service of a disclosure warrant issued by a U.S. court, arguing that the warrant constituted an unlawful extraterritorial application of the Stored Communications Act (SCA) under which the disclosure warrant was provided for.[338] A generally applicable Supreme Court judgment would be problematic whichever party prevailed at the end, because it would either force the U.S. internet service providers to disclose user information wherever in the world that the information was stored, or it would foreclose the access of U.S. law enforcement to user data stored abroad in all cases, even when the crime and suspect was closely connected to the U.S.

The Cloud Act was drafted and passed following debates that focused on whether data location could be a feasible determinant of which state had prescriptive and enforcement jurisdiction over the compelled disclosure by law enforcement of user data with regard to cloud computing based services. Major U.S. service providers were apprehensive of the penalties they might face if they disclosed to U.S. law enforcement (upon a warrant from a U.S. court) data located in other countries that had strict rules on international personal data transfers. The EU General Data Protection Regulation (GDPR)[339] in particular proved to be very problematic due to the fact that (i) Europe was one of the major export markets of major U.S. cloud providers, (ii) a combination of court cases (such as *Google Spain*[340]) that strengthened the reach of the EU personal data protection rules to a broader range of service provider activity and the consolidation of the view in Europe that personal data protection rules should exclusively regulate law enforcement cooperation with third countries[341], and (iii) the GDPR prescribed very substantial penalties for violation of third country transfer rules.[342] American law enforcement worried that without the authority to compel disclosure of data located abroad, it would not be possible to collect evidence in many crimes that exclusively concerned the United States or U.S. persons, since Mutual Legal Assistance Treaties were not efficient in the timely collection of electronic evidence.[343] The government of the United Kingdom also had a prominent voice in these discussions, and they

337 *United States v. Microsoft Corporation,* 584 U.S. ___ (2018). (https://www.oyez.org/cases/2017/17-2).

338 18 U.S.C. § 2703, (https://www.law.cornell.edu/uscode/text/18/2703).

339 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, OJ L 119, 4.5.2016, p. 1–88, (http://data.europa.eu/eli/reg/2016/679/oj).

340 *Google Spain v AEPD and Mario Costeja González,* Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

341 The latter can be evidenced in the (ex) Article 29 Working Party's position related to the Council of Europe Budapest Cybercrime Convention. The WP29 strongly advocated against any interpretation of Articles 18 and 32 of that Convention that might undermine the application of the GDPR's data transfer regime to criminal law enforcement cooperation with third countries. See EUROPEAN COMMISSION ARTICLE 29 WORKING PARTY, *Data Protection and Privacy Aspects of Cross-Border Access to Electronic Evidence,* statement of 29 November 2017 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

342 See B. SMITH, *Written Testimony of Brad Smith President and Chief Legal Officer, Microsoft Corporation submitted the U.S. Senate Subcommittee on Crime and Terrorism,* 10 May 2017 (https://www.judiciary.senate.gov/download/05-24-17-smith-testimony).

advocated for either setting up a bilateral framework that allowed the two governments to directly request the disclosure of user data from service providers in cases where the crime was exclusively related to one of the states and their residents, wherever the data is located.[344] As to contributions from academia, two voices distinguished themselves. Jennifer Daskal, who was one of the main proponent of the Cloud Act in academia, argued that the nature of data increasingly created a discrepancy between the outcome that a data location based territorial rule is expected to yield in terms of a stratification between the several sovereign interests involved, and the real outcome created when that territorial rule is applied and enforced in practice.[345] Daskal argued that the solution necessarily required a multilateral approach at the international level. *Contra* Daskal, Andrew Woods turned to conflict of laws methodologies for the solution. According to his point of view, data does not offer a special difficulty, and the conflict of laws discipline has the necessary tools in its disposal to deal with the conflicting interests, largely on a case by case basis, and to create new guiding principles to equitably distribute prescriptive and enforcement powers to the sovereigns involved. Woods suggested that the abovementioned discrepancies between expected outcomes and real outcomes be overcome by courts employing some type of governmental interest analysis.[346] For American commentators, reference to a governmental/state interest analysis is informed by American common law that incorporates various choice-of-law methodologies developed as a result of the so-called American Conflicts Revolution.[347] In Europe, on the other hand, there is generally less doctrinal ground on which courts can explicitly analyze the conflicting interests on a case by case basis.

The Cloud Act creates two new statutory rights for service providers. 18 U.S.C. §2702(b)(9) stipulates that service providers may voluntarily disclose the contents of communications held in electronic storage, or carried or maintained by the provider to foreign governments upon request given that the foreign government is party to an executive agreement pursuant to §2523. §2702(c)(7) provides the same right in relation to customer records. Direct disclosures of user content data to foreign governments were explicitly forbidden under the previous version of the law. The second statutory right is the right to file a motion to quash or modify a warrant obtained from a U.S. court for disclosure of user data *only if* the disclosure would require the service provider to violate the law of a foreign government qualified by executive agreement *and* the subject of the warrant is not a U.S. person or U.S. resident (§2703(h)(2)). Upon this motion, the court will make a «comity

343 «the MLA process can lack the requisite efficiency for time-sensitive investigations and other emergencies, making it an impractical alternative to SCA warrants in many cases» B. WIEGMAN, *Statement of Brad Wiegman U.S. Deputy Ass't Att'y Gen. before the U.S. Senate Subcommittee on Crime and Terrorism*, 24 May 2017, p.6 (https://www.judiciary.senate.gov/download/05-24-17-wiegmann-testimony); «[MLATs] are widely regarded in the law enforcement community as a wholly ineffective alternative to obtaining evidence.» R. LITTLEHALE, *Written Statement by Richard Littlehale Special Agent in Charge Tennessee Bureau of Investigation submitted to the United States House of Representatives Committee on the Judiciary*, June 15, 2017, p. 2 (https://judiciary.house.gov/wp-content/uploads/2017/06/Littlehale-Testimony.pdf).

344 P. MCGUINNESS, *Written Testimony of Mr Paddy McGuinness United Kingdom Deputy National Security Adviser submitted the U.S. Senate Subcommittee on Crime and Terrorism*, 10 May 2017, (https://www.judiciary.senate.gov/download/05-24-17-mcguinness-testimony).

345 J. DASKAL, *The Un-Territoriality of Data,* in *YLJ*, 2005, p. 326.

346 A. K. WOODS, *Against Data Exceptionalism,* in *SLR*, 2016, p.729.

347 S. C. SYMEONIDES, *The American Choice-of-Law Revolution: Past, Present and Future,* Leiden, 2006.

analysis» by considering the specific factors provided under §2703(h)(3). This comity analysis that is done upon motion (which I call "*comity-upon-request*" in line with the argument of this paper) is explicitly distinguished in the text of law from the ordinary comity doctrine under American common law. Also, service providers may notify qualified foreign governments in cases where a disclosure of data process concerns data belonging to their nationals or residents, which would be illegal under the previous version of the law.

American critics of the new law have mostly focused on another set of provisions in the law that relax the SCA's previous categorical ban on the disclosure of user content data to foreign law enforcement by allowing U.S. service providers to disclose user content to criminal justice authorities of foreign governments that have signed an executive agreement with the U.S. government.[348] These critics fear that direct foreign government access to U.S. provider held user data could be used to circumvent U.S. rules regarding user privacy, since the executive agreement framework does not require foreign legal systems that will be authorized to have a probable cause standard for compelled search and seizure equivalent to the U.S. standard and the data acquired could end up being used in U.S. lawsuits, which is especially problematic if data regarding U.S. persons are also acquired in the process although the executive agreement framework requires foreign governments to adopt data minimization procedures to filter out and eliminate data that may be connected to U.S. persons.[349] These critics also point at the danger that the relaxation of the absolute disclosure ban may result in "bad states" accessing data of users.

3. The important privacy and evidence-standard implications of the Cloud Act notwithstanding, in this paper I want to focus instead on the *comity-upon-request* rule and its possible motivations and logic. I argue that the *comity-upon-request* rule might be motivated by an information problem that is the result of an effort to recalibrate and use conflict of laws methodology to facilitate corporate access to a global data storage and processing market. As data storage is a commodity in these markets, the fact that data location (which is an inalienable physical property of data storage) is imbued with jurisdictional claims by legal systems creates compliance-related costs but also costs related to legal uncertainty. A legal system, which in turn seeks to facilitate its domestic corporations access to a foreign data (storage) market can forfeit a part of its own prescriptive and enforcement authority in order to reduce the potential for conflict of laws that create such costs; but such a forfeiture has its own social and political costs as forfeiture of authority (which corresponds to deference to a foreign legal system) means a decrease in the state's

348 18 U.S.C. §2523, (http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2523&num=0&edition=prelim).

349 Electronic Frontier Foundation: C. FISCHER, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data,* 8 February 2018 (https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data); D. RUIZ, *Responsibility Deflected, the CLOUD Act Passes,* 22 March 2018, (https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes); K. RODRIGUEZ, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom,* 9 April 2018, (https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom); American Civil Liberties Union (ACLU): N. S. GULIANI, N. SHAH, *Proposed CLOUD Act Would Let Bad Foreign Governments Demand Data From US Companies Without Checks and Balances*, 19 March 2018, (https://www.aclu.org/blog/privacy-technology/consumer-privacy/proposed-cloud-act-would-let-bad-foreign-governments-demand); Electronic Privacy Information Center (EPIC): *The CLOUD A*ct (https://epic.org/privacy/cloud-act/).

capacity to realize public policy, e.g. prosecuting child pornography or drug sales as in the *Microsoft* case.

On the other hand, testimonial evidence suggests that although, theoretically, the risk of conflict of laws is high in scenarios where more than one legal system has a veritable jurisdictional claim on the activity in question, in practice, U.S. service providers have not met substantial opposition by other states when they were disclosing user data stored on their territories to U.S. law enforcement; that is until the U.S. service providers *themselves* started objecting to the practice.[350] If this was indeed the case in practice, then facilitating global market access via forfeiting prescriptive authority in anticipation of (theoretical) costs of conflict of laws might possibly be overcompensating this risk at a high social and political cost.

Herein lies what I call the information problem. Due to the lack of information as to the possibility of foreign legal systems claiming (or not claiming) jurisdiction where they have typically have not (or have), which partly results from the fact that the matter of international cooperation in law enforcement is typically managed in the bureaucratic level that is susceptible to capricious changes in practice, the legal system (both the legislative and the courts) cannot efficiently calculate the costs to corporations of conflicts of laws and thus balance *ex ante* these costs with the costs of forfeiture of authority. The *comity-upon-request* solution thus makes use of the corporation's own intelligence, know-how, and legal resources to assess scenarios when a U.S. court's warrant for worldwide disclosure of user data would be opposed by a foreign legal system, and require the U.S. to forfeit authority only in these scenarios but not in others where such a warrant could be fulfilled without opposition.

The information problem introduced above can be analyzed in finer detail to assess the merits of the proposed solutions and predict future uses of regimes similar to that in the Cloud Act. I propose a preliminary analysis of the information problem suggesting that legislators and government organs are faced with three types of information problems when deciding whether to assert prescriptive and enforcement jurisdiction in cases concerning data flows:

The three information problems

The general political information problem: Following the failure of activity location as a proxy, courts and the State cannot determine the extent of its interests affected in a given conflict. The corporate actor is "closer" to the conflict and its (economic and political) fallout.

The special political information problem: In the light of its role vis-à-vis the corporate actor, the State cannot determine with high certainty the outcome relative to the interests of the corporate actor, and application of proxy rules do not provide enough flexibility to the State to achieve results in line with the State's role vis-à-vis the corporate actor.

The judicial information problem: The courts do not have sufficient information to

350 See B. SMITH, *Written Testimony of Brad Smith President and Chief Legal Officer, Microsoft Corporation submitted the U.S. Senate Subcommittee on Crime and Terrorism*, cit.

ascertain the exact outcome relative to interests at stake preferred by the political branches. This is not a new problem, but is exacerbated by the dynamics of the modern economy, and increased rate of technological change that makes policy inherent in certain rules obsolete at a rate that the political branches cannot keep pace.

4. My interpretation of the motivations of the Cloud Act is based on two assumptions based on observations that will be discussed in this paper. The first assumption is that the facilitation of global market entry for corporate subjects is genuinely identified as a central interest of the state in the context of the application of conflict of laws methodology. The second assumption is that connecting factors such as data location can be thought of having intrinsic links with certain interests, to the effect that a shift in the perception of its interests would be a motivation for a state to abandon it for the sake of a connecting factor that is more instrumental to its newly perceived interests. I shall call this second assumption the proxy theory of connecting factors.

If these assumptions hold and my interpretation of the Cloud Act framework is workable, then this might yield insight helpful to predict future directions for the regulation of data flows and big data applications from a perspective different from substantive privacy law by placing the issue in a broader context of globalization and global governance. The use of conflict of laws methodology, including doctrines of comity, to facilitate corporations' participation in global denationalized markets by enabling corporations to release themselves from national jurisdictions is discussed in the literature and advocated by some commentators to be the correct path that the conflict of laws/private international law scholarship should take to remain relevant in the contemporary legal environment, where non-state private actors are competing with states for legitimacy in norm creation.[351]

The approach I am advocating will also help filling a gap in critical commentary of the ongoing trend of "privatization" of data flow regulation, such that directed at "the right to be forgotten" regime set after the ECJ decision in the *Google Spain* case. For instance, comments coming from the Electronic Frontier Foundation (EFF) regarding the Cloud Act and similar proposals in Europe appear to suggest that the "privatization" of the legal safeguards and assessment processes in both sides of the Atlantic have their basis in a lack of political will to uphold digital privacy rights. An innate inclination to surveil its citizenry that is frequently attributed to the nation state is a usual suspect in these critiques, however, in light of the structural and procedural distinction between criminal law instruments and national security instruments, and the hybrid character of these novel types of regulation, this explanation seems unsatisfactory. Thus, an explanation that accounts for the motivations for such policies of "privatization" and how they

351 R. WAI, *Transnational Liftoff and Juridical Touchdown: The Regulatory Function of Private International Law in an Era of Globalization,* in *CJTL*, 2002, p. 209; H. MUIR-WATT, *Private International Law Beyond the Schism,* in *TLT*, 2011, p. 347. I additionally argue that recent developments in the U.S. yields further evidence of the existence of a global market access facilitation motif also in the field of U.S. personal jurisdiction, whereby the exposure of large multinational companies to litigation in state courts are being significantly lowered as the U.S. Supreme Court adopts a stricter general/specific personal jurisdiction distinction akin to the Brussels (recast) regime in the EU, however made even more advantageous to multinationals due to specific additional doctrines of U.S. personal jurisdiction law**.**

are legitimized through joint appeals to both commercial necessities and security threats without relying too much on essentialist assumptions about the state could be useful.

5. The following factors can be identified as main governmental interests that could clash with each other, requiring a novel approach to jurisdictional rules that might make use of "privatizing" frameworks, such as comity-upon-request in the Cloud Act.

(1) Securitization of private data flows: The last decade has seen a proliferation of perceived online threats emanating from private persons or private groups. Social media and other web 2.0 applications have enabled certain types of private behavior that threatens public safety such as online radicalization and/or the spreading of disinformation regarding to all kinds of societal events. The perceived increase of such threats combined with the fact that the relevant medium of the threat is increasingly based on cloud computing technology, creates a motive for states that I call the "securitization" of private data flows. Securitization of cross-border communications is of course nothing new, it is arguably as old as the invention of writing systems, but at the very least it predates the popularization of cloud computing.[352] Instead, what I refer to by the securitization of data flows is a distinct phenomenon. I mean the perception of digital communications as a medium that is extremely conducive to hostile activities against the state and/or social order due to its enormous capacity to reach private citizens and the public domain. This perception guides the stance of the security apparatus of the state including criminal justice, national security, and military departments.[353]

The threat that securitization of private data flows envisions is typically derived from communications directed to persons located within the territory of the state, originating from persons, or groups, that may be located inside or outside of the territory of the state. From this perspective, the use of virtual networks, shell user accounts, automated bots, or other clandestine techniques render determinations of applicable law based on physical origin of the communication irrelevant to the state interest that is impacted by the communication, while the fortuitous connection between the communication and origin state offer poor justification for exclusively

352 Samuel Morland, an officer in the Royal Mail under Oliver Cromwell, on surveillance of private letters: «A skillful prince ought to make a watchtower of his general post office and there place such careful sentinels as that by their care and diligence he may have a constant view of all that passes. By the frequent inspection of letters a king soon know the temper of all his principle and active subjects.» T. SIMPSON, *Liberty and Surveillance: What Governments and Private Corporations Know About You?*, CIS Occasional Paper 162, 2018, p. 7, (https://www.cis.org.au/app/uploads/2018/01/op162.pdf).

353 Securitization of data flows happen on a wide continuum that extends from policing petty criminality to conducting counterterrorism and at the extreme, militarization of cyberspace. In June 2017, following a long period of efforts and discussions since 2004, the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security failed to finalize a document concerning how international law applies to States' use of ICTs, due to a lack of consensus on whether malicious use of ICTs could be considered as an "armed attack" as a matter of *jus ad bello*, and whether humanitarian law would apply to ICT-based operations of security forces. A. M. SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, 4 July 2017, (lawfareblog.com, archived at https://perma.cc/5QZY-GUVD). Also see U.S. envoy to the GGE Michele G. Markoff's statement concerning the failure to reach a consensus: M. G. MARKOFF, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, 23 June 2017, (https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm).

determining prescriptive jurisdiction on the basis of location.[354] This puts the pressure on judicial systems to claim prescriptive and enforcement authority based on effects felt within their territories (inasmuch as territoriality remains as a proxy for a great majority of other state interests). This pressure may sometimes result in a government position that is unilateralist (some may say realist):

> «Congress did not enact a disclosure scheme that a U.S. provider could nullify by the expedient of shifting data to storage devices that it locates over the border. To allow that result would permit a private provider in the United States to thwart Section 2703's critical role in assisting law enforcement to combat terrorism and crime.» (Brief for the United States in *U.S.* v. *Microsoft*).[355]

> «the possibility of a future conflict between U.S. and foreign law does not change the best construction of an important domestic law enforcement and counterterrorism tool enacted more than 30 years ago.» (ibid.)[356]

> «it takes on average about 10 months to obtain communications from a U.S. Provider in response to an MLAT [Mutual Legal Assistance Treaty] request, and can take even longer. This is not timely enough to be useful to the U.K.'s law enforcement when they are trying to anticipate and head off terrorist and security threats or stop ongoing crimes such as drug trafficking and child abuse.» (Amicus Brief for the U.K in *U.S v. Microsoft*).[357]

The last testimony regarding the failure of MLATs as an efficient instrument for cross-border cooperation is a common theme that appears in arguments surrounding unilateral compulsion of service providers to disclose user data, and parties to this debate appear to have conflicting views on their value. For instance, while the U.S. and U.K. government agencies seem to generally complain of their unsuitability faced with the large volume and immediate nature of online threats, the Irish government seems confident of the efficiency of the U.S.–Ireland MLAT system, and the

354 For instance, the U.S. deputy assistant attorney general's testimony before a Senate hearing on law enforcement access to data stored abroad represents such a perspective: «The impacted [by the Second Circuit decision allowing Microsoft to not disclose user data stored in Ireland] investigations run the gamut – from child exploitation and human trafficking, to firearms and drug smuggling, to tax fraud, computer fraud, and identity theft. These cases directly affect public safety and may even affect national security. While the most obvious impact of the Microsoft decision may be to frustrate investigations of foreign nationals targeting U.S. victims, these examples make clear that the Microsoft decision also thwarts or delays investigations even where the victim, the offender, and the account holder are all within the United States.» B. WIEGMAN, *Statement of Brad Wiegman U.S. Deputy Ass't Att'y Gen. before the U.S. Senate Subcommittee on Crime and Terrorism*, cit., p. 6.

355 *Brief for the United States* in *U.S.* v. *Microsoft*, 6 December 2017, p. 43 (https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf).

356 *Id.* p. 52.

357 *Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as amicus curiae* in *U.S. v.* Microsoft, 13 December 2017, p. 11 (https://www.supremecourt.gov/DocketPDF/17/17-2/23693/20171213140104710_17-2%20-%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland.pdf).

European Data Protection Board (EDPB) seem to consider MLATs to be central to the GDPR's framework for data transfers to third countries in the context of law enforcement cooperation.[358]

Thus, the sense of urgency produced by a securitization posture regarding private data flows and the perceived inefficiency of bilateral cooperation agreements may create a motive for unilateral claims to prescriptive and enforcement jurisdiction, or push governments to advocate in the domestic and international level jurisdictional rules that make use of effects-based connecting factors rather than data (and/or processing) location-based ones. In this context, rules that assign prescriptive jurisdiction based on nationality or residency of the user may be interpreted to contain an assumption that communication originating from these persons have some effect on the territory and subjects of the state by virtue of the connections these persons have with the state and its society.

It should not be surprising that in determining an extraterritorial jurisdiction "strategy", governments consider international "political" costs of their choice, which are typically envisioned as a scenario of reciprocation of the strategy by foreign states. In the context of cyberspace, the tension between states' capacity to engage in unilateral action with impunity and the potential benefits of an international rule-of-law has been a treated as important issue in since the beginnings of "cyberlaw" scholarship.[359] However, in relation to digital markets, the securitization of data flows bring with it demands for alignment between international trade strategies and national security strategies, which is not very conducive to achieving a solution based on wide international cooperation.[360]

(2) Facilitation of global market access: Admittedly at this point I can only offer circumstantial evidence regarding the existence of a coherent conception of facilitation of global market access as a governmental interest to be taken into consideration when the administration or courts decide on the exercise of extraterritorial prescriptive jurisdiction, *distinct from the customary*

358 Cf. *Brief for the United States in U.S v. Microsoft*: «to the extent that an MLAT covers the requested data in a particular case, the process can be slow and uncertain, often taking many months or even years to generate results» (pp. 44-45), *Brief for the Government of the U.K in U.S v. Microsoft as Amicus Curiae.* (see relevant quote above in text), *Brief for Ireland in U.S v. Microsoft as Amicus Curiae*: «Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and is ready to consider, as expeditiously as possible, a request under the MLAT, if and when it be made.» (p. 8), and EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018: «In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.» (p. 5, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en)

359 M. HILDEBRANDT, *Extraterritorial Jurisdiction to Enforce in Cyberspace?: Bodin, Schmitt, Grotius in Cyberspace*, in *UTLJ*, 2013, p. 196.

360 In the context of cloud computing services, one factor leading to such an alignment may be the national security implications of powering governmental and public services with private cloud computing services. E.g. see V. KUNDRA, *Federal Cloud Computing Strategy*, 8 February 2011, (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf). In the U.S.A., this demand for alignment manifests itself in discussions regarding extraterritorial prescriptive jurisdiction in the form what I call the "bad state" reciprocity paradox. Simply put, the "paradox" arises from asking the question of «would we like if the governments of [insert "bad state" of choice] asserted their jurisdictional authority in the same way?" for each possible solution for exercising jurisdiction in cyberspace and reaching the answer "no" each time. Even a pure territorial solution based on data location cannot escape the paradox, as «that would create data havens for malign activity».

deference shown to the foreign state's sovereign right of regulating commerce in its own territory.

Nevertheless, at least in the context of the U.S., there seems to exist a doctrinal basis to consider such an interest, if found to exist, in to the international comity consideration regarding the extraterritorial application of U.S. law.[361] It has been observed that courts, including the U.S. Supreme Court have considered the United States' interest in deferring to foreign law by way of the doctrine of comity for the sake of «harmony […] needed in today's highly interdependent commercial world».[362] Also, it is stated in the Restatement (Third) of Foreign Relations Law, which compiles a review of and comments on the valid American common law in matters related to foreign relations including prescriptive jurisdiction, that in deciding whether a state (or the federal government) may exercise prescriptive jurisdiction a court will evaluate, *inter alia,* «the importance of the regulation to the international political, legal, *or economic* system».[363] Perhaps more significantly, the comity analysis prescribed in the Cloud Act itself, which will be undertaken by the court upon a motion to quash filed by the provider, stipulates that the court shall take into account, *inter alia* «the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider.»[364] Moreover, the Cloud Act requires foreign states to «[demonstrate] a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet» in order to be eligible for entering into an executive agreement with the U.S. government that would authorize that state to order U.S. service providers to disclose certain user data to their law enforcement authorities and would make them eligible for benefiting from the comity analysis prescribed in the Act.[365]

Concerning the particular context of cloud service provision and export, it appears that the U.S. government perceives conflict of laws as an important barrier for U.S. companies to exploit global markets. The U.S. Department of Commerce has assessed foreign law compliance issues,

361 Although not directly relevant to the question if prescriptive jurisdiction, this point is further evidenced in the field of personal jurisdiction. Recent U.S. Supreme Court decisions in *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915 (2011) and *Daimler AG v. Bauman* 571 U.S. ___ (2014) have effectively shifted the focus of the criteria required for a court to claim general personal jurisdiction over a transnational corporation from the degree of commercial presence a corporation has within the territory of a state *objectively* determined, to the degree of presence *subjectively* determined, i.e. presence relative to the overall size and organization of the company itself. The result is that a very large transnational corporation can escape general personal jurisdiction of a court even in cases where its operations in the forum state are worth billions of dollars. The main aim behind this change is shielding large multistate (or multinational) corporations from forum shopping, thus enabling them to enter foreign markets without attracting litigation risks in the forums of that market, except in cases where the dispute arises from the activity located in that host state, and only for damages that are suffered in that host state. General personal jurisdiction under this scheme is only allowed in the residence or headquarter of the corporation, and in practice companies can manage litigation risk through intelligent corporate structuring and by objecting jurisdiction on the basis of *forum non conveniens*. The overall result is that the adjudicatory powers of the state (and the access to justice of potential plaintiffs) are curtailed for the benefit of enabling easier market access for corporate subjects.

362 *F. Hoffmann-La Roche Ltd. v. Empagran S.A*. 542 U.S. 144, 164–65 (2004).

363 AMERICAN LAW INSTITUTE, *Restatement (Third) of Foreign Relations Law of the United States*, § 403 (1987, October 2017 Update), (emphasis added).

364 18 U.S.C. §2703(h)(3)(C).

365 18 U.S.C. §2523(b)(1)(B)(vi).

including particularly data transfer and data localization requirements as the primary international competitiveness issues facing U.S. cloud computing service providers:

> «Key International Competitiveness Issues
> When entering or expanding into international markets, U.S. cloud service providers might face some of the following market challenges:
> 1)Data localization restrictions requiring data to be stored, processed or handled in the same country where it originated.
> 2)Compliance with foreign laws establishing measures regarding how certain data maybe transferred across borders.
> 3) Being required to have a local presence in-market (e.g., distributor, sales office, business representative, joint venture partner, etc.) could make a significant difference in a company's abilities to do business, especially with the public sector.
> 4) Other competitive ness issues such as licensing requirements, and cyber security and restrictive procurement policies.»[366]

(3) Protection of the privacy rights of subjects: Although an important interest of the state, this interest is not directly relevant to the question of deference to foreign law in the context of the comity-upon-request framework of the Cloud Act. However, the foreign state's interest in the protection of the privacy rights of its citizens and residents plays a direct role in the comity assessment. The consideration of privacy rights of subjects may also be indirectly relevant in a comity analysis if the "political" consequences of exercising extraterritorial prescriptive jurisdiction are (somehow) taken into account, e.g. the foreign state reciprocating by ordering service providers to disclose data of users resident in the first state. This issue will not be detailed in this paper.

(4) IT protectionism: This interest does not play a role from the perspective of the U.S. due to the already dominant position of U.S. service providers (and the weak competition these providers face from foreign providers in the U.S. market), however for other governments protecting domestic providers from the complete domination of their national markets by foreign providers may be a real motivation which could lead the passing of privacy laws that encourage or require data localization as a matter of fact, if not by law, benefiting domestic providers in the process.[367] Nevertheless, protectionist motivations may be also thought as overlapping with the securitization trend and the facilitation motivation discussed above, as foreign domination of the domestic market could make it difficult for domestic service providers to thrive, and foreign control of a large volume of citizen (and public) data may be perceived as a security threat.

How a protectionist interest may interact with the law of jurisdiction, especially in legal systems which ostensibly reject openly protectionist trade policies is must play an important part in any theory of how globalization in computing/data services are affecting the use of conflict of laws

366 U.S. DEPARTMENT OF COMMERCE INTERNATIONAL TRADE ADMINISTRATION, *2017 Top Markets Report Cloud Computing Sector Snapshot*, p. 2, (https://www.trade.gov/topmarkets/pdf/Sector%20Snapshot%20Cloud%20Computing%202017.pdf).

367 For a recent example, see V. GOEL, *India Pushes Back Against Tech 'Colonization' by Internet Giants*, NYT Online, 1 September 2018, (https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html?action=click&module=Top%20Stories&pgtype=Homepage).

doctrines. However, as this paper is focused on the use of the particular use of comity in the Cloud Act, the protectionist motive will not be discussed in detail.

6. It has been suggested by various commentators that the fundamental reason that causes data location to be a problematic connecting factor is that in the case of data (as opposed to physical things or persons) location does not correlate with the existence of legitimate interests of the state governing that location to an extent sufficient enough to justify the exclusive prescriptive authority of the state in question regarding the regulation of the behavior related to that data.[368] It appears in the light of recent legislation and official commentary either side of the Atlantic that there is a divergence on the acceptance of this idea, at least in the policy making level. In the U.S., the recently passed Cloud Act provides for an unusual framework for international cooperation that envisions both executive-level international cooperation and collaboration between transnational service providers and (foreign) law enforcement. This framework acknowledges that deference to foreign law is inevitable to uphold the existing global data flows and value chains created by these, but it is also firm in its adoption of the idea suggested above.

On the other hand, in Europe, the recent entry into force of the GDPR with its strict rules for data transfers to third countries and extensive claim to prescriptive jurisdiction seems to represent a maximalist approach to prescriptive jurisdiction that rejects complete irrelevancy of data location as proposed by the abovementioned view. It appears that in current EU data protection law, the location of data is thought to correlate with a bundle of core interests that are protected by the most hallowed of norms, *viz.* the sovereign's right to non-intervention, and the user's fundamental right to privacy. Moreover, the from the perspective of EU law, the unfettered enjoyment of the latter right and the Union's interest in upholding it justifies extraterritorial application of EU law – this time by way of the user's residence as a connecting factor. The line, however, is drawn at extraterritorial enforcement, which represents a more traditional understanding of the difference between prescriptive jurisdiction and enforcement jurisdiction in the context of international law.

On the day of the entry into force of the GDPR, two Guidelines were adopted by the new European Data Privacy Board that replaced the Article 29 Working Party. Unsurprisingly, both concerned transfer of data to third countries. The second, Guidelines 2/2018, directly foreclosed the possibility that Article 49 could provide a basis for cooperation of the data controller with third country law enforcement, a possibility that was suggested by the European Commission in its amicus brief in *Microsoft*:[369]

368 E.g. see J. DASKAL, *Borders and Bits*, in *VLR*, 2018, p. 226; D. SVANTESSON, *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, AJIL Unbound*, 2015, p. 72. For a view arguing that territory never had much representative power regarding state interest see P. D. SZIGETI, *The Illusion of Territorial Jurisdiction,* in *TILJ*, 2017, p. 371.

369 «The legitimate interest [under GDPR art. 49(1)] could, again, be the interest of the controller in not being subject to legal action in a non- EU state» *Brief of the European Commission on Behalf of the European Union as Amicus Curiae in U.S. v. Microsoft*, 13 December 2017, p.16, but also «It should also be noted, however, that Article 49 is entitled "Derogations for specific situations." Therefore, these grounds are to be interpreted strictly» (ibid. at 17) (https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

> «The GDPR introduces a new provision in Article 48 that needs to be taken into account when considering transfers of personal data. Article 48 and the corresponding recital 115 provide that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Therefore, a transfer in response to a decision from third country authorities is in any case only lawful, if in line with the conditions set out in Chapter V. […] In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), *EU companies should generally refuse direct requests* and refer the requesting third country authority to existing MLAT or agreement.»[370]

Similarly, an amici brief for MEPs in *Microsoft*, whose *amici* includes Viviane Redding, the EU commissioner that initiated the legislative work for the GDPR, and Jan Philipp Albrecht, the parliamentary rapporteur for the GDPR and the U.S.-EU "Umbrella Agreement", took a strict view of the exclusivity of the Art. 48 rule requiring an international agreement basis for data disclosure to third country law enforcement organs and categorically denied the applicability of the Article 49(1) "important reasons of public interest" exception to disclosures to foreign law enforcement.[371]

This difference in views poses a problem for transnational service providers which deal in very large volumes of transatlantic data transfers. As purveyors and movers of data and storage thereof, it appears that it would be more in the interest of service providers if data location would not be representative of the existence of such a bundle of core governmental interests. As a significant feature of their business models and economies of operation depends on global transfers of data, it can be conjectured that the less a change in data location signifies a change in corporate legal obligations, the better it is for the corporation. On the other hand, if it is not possible to completely disassociate governmental interest from data location, another beneficial option would be curtailing extraterritorial application to avoid conflicts of law for the sake of foreseeability. Both configurations can theoretically be achieved through international intergovernmental cooperation, but the latter configuration may also arise through unilateral actions of states under certain circumstances where governmental interest is found to be best served with prescriptive self-restraint.

States are jealous of their prescriptive powers, and they will not forfeit them lightly. States may voluntarily limit their extraterritorial prescriptive powers when they recognize an interest in deferring to the sovereign rights of other states, notwithstanding the theoretical legal problem of whether there is a norm of international law that require them to do so. For example, it seems that the United States courts recognizes an interest in upholding the «highly interdependent global market» by refusing to apply U.S. law in cases where legitimate foreign interests call for the application of foreign law, or by deferring to private choice-of-law or arbitration agreements at the

370 EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, cit., p. 5 (emphasis added).

371 *Brief of amici curiae Jan Philipp Albrecht, Sophie In'T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, members of the European Parliament* in *U.S. v. Microsoft*, 18 January 2017, p.17, (https://www.supremecourt.gov/DocketPDF/17/17-2/28328/20180118155453076_17-2%20bsac%20Jan%20Philipp%20Albrecht.pdf).

expense of the authority to enforce public policy.[372] Although the issue is far from settled in U.S. law, it is notable that in his amicus brief in *Microsoft*, the U.N. Special Rapporteur on the Right to Privacy seemed to espouse the view that considered deference to the foreign law via the doctrine of international comity as a requirement of fostering commercial relationships between nations, citing the *Empagran* decision:

> «Respect for foreign sovereigns is not, however, premised solely on an abstract notion of sovereign independence. Rather, it is a practical element of fostering positive diplomatic and commercial relationships between nations and preventing "international discord." Nor is comity solely the concern of the judiciary. As this Court observed in F. Hoffmann-La Roche Ltd. v. Empagran S.A., it is assumed "that legislators take account of the legitimate sovereign interests of other nations when they write American laws, [which] helps the potentially conflicting laws of different nations work together in harmony – a harmony particularly needed in today's highly interdependent commercial world." Executive agencies are similarly expected to consider the interests of foreign sovereigns when enforcing domestic laws.» [citations omitted][373]

7. A common theme found in critiques of the Court of Appeals for the Second Circuit's decision for Microsoft[374] (which was appealed to the Supreme Court and had found that the FBI's use of the disclosure warrant was indeed extraterritorial based on data location and therefore unlawful) and Microsoft's pure territorialist views on data location and prescriptive jurisdiction is the argument that data location does not serve as a good proxy for the state interests involved in the dispute, rendering the use of data location as a connecting factor a bad conflict of laws practice. At the core of this argument is the premise that all connecting factors, especially those that are based on the notion of territoriality, are proxies for certain preferred stratifications of the interests (of relevant parties, sovereigns, and third parties) being affected by the legal event in question. According to this, rules concerning adjudicative, prescriptive and enforcement jurisdiction all operate through concepts that encapsulate the postulated interests of actors. Examples are territory of a sovereign, nationality of an actor, location of an immovable, place of contracting, using a satellite uplink, advertising in a certain language, participating in a commercial fair. In other words what these kinds of factors and concepts achieve is to allow courts to favor the interests of one party (or sovereign, or third party) over another by simply making a binary choice as to the existence of the connecting factor, thus keeping the question strictly within the sphere of legal analysis, by

372 *F. Hoffman-La Roche, Ltd. v. Empagran, S.A* 542 U.S. 155 (2004) cited in J.R. PAUL, *The Transformation of International Comity*, in *LCP*, 2008, p. 36. Paul critiques the development of the doctrine of international comity in U.S. courts and argues that it is increasingly used to relinquish state authority to prescribe public policy not only in deference to foreign sovereigns, but more importantly in deference to the global market itself.

373 *Brief Amicus Curiae of U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in Support of Neither Party* in *U.S. v. Microsoft*, 13 December 2017, pp. 32-33, (https://www.supremecourt.gov/DocketPDF/17/17-2/24918/20171222120327043_35632%20pdf%20Krishnamurthy.pdf)

374 *Microsoft Corp. v. United States*, 2nd Cir., 14 June 2016, vacated by Supreme Court as *United States v. Microsoft Corporation,* 584 U.S. ___ (2018).

having the court not to engage into a technical discussion of all the interests at stake in the conflict and stratifying them, which is a political action in nature.

For instance, when a court decides that the law of country X applies and not country Y, because the performance of the contract provision in question was to take place within the territory of country X, the conflict rule that the court is applying, i.e. that the law of the place of performance of the contractual obligation will apply, solves the balancing of interests problem by reducing the question of competing interests to a relatively less controversial, less complex, and much more easily observable factual finding that the court can make based on much less evidence and technical expertise compared to actually identifying and calculate the interests at play. The binary choice (existence or non-existence of performance obligation in X or Y) essentially provides two scenarios in which the stratification of interests are "pre-calibrated" by the legislator, e.g. in our scenario of the contract, it is decided by the legislator *ex ante* to the dispute that the interests of the state in whose territory the performance will take place trumps that of the state which is connected to the legal relationship in other ways, with regards to the regulation of the contract. The pre-calibration of this preference for the interests of the state in whose the territory the contract is performed is applied generally and may include cases in which the normative concerns of the legislator would actually point to the other state's law to be applied, but the benefits of the general rule is assumed to outset the occasional misappropriation. The view that such *ex ante* pre-calibration is prone to error in and is essentially arbitrary has formed the basis of what is called the American Conflicts Revolution, and the rise of "governmental interest analysis" as an alternative *ex post facto* interest stratification method for courts to choose the applicable law in the United States.[375] In Europe, where active interest analysis by the courts was theoretically undesirable due to its political nature, courts have nonetheless used *ordre public* exceptions and other escape mechanisms included in the system based on the pre-calibrated rules to bridge cases in which they thought the conflict of laws rules yielded misappropriation.

The proxy theory is compatible and favorable to the hypothesis propounded in this work, that there is an informational problem that underlies the development of the "privatizing" solutions in global data flow regulation, and in particular, the *comity-upon-request* regime brought by the Cloud Act in the U.S. The informational problem is more acute if it is assumed that facilitating or ensuring global market access for domestic capital has become a central interest of the State. This would mean that determining the state's interests in a conflict case now (to a much greater extent) entails assessment of market responses to the global regulatory reach of the of the State. In the context of data flows, such assessment increasingly requires specialized technical knowledge and insights because of the rapidly changing and disruptive nature of the technology sector. Courts no longer can rely on proxy concepts to make an interest analysis that can properly account for the State's interest flowing from its new role. They simply lack the information, and the application of the former proxies can lead to unintended results. Thus, the solution to this problem is to "outsource" the information gathering to the corporations that can avoid rules that are "counterproductive" in the light of the State's new central interest through choice of law, choice of forum, or arbitration agreements; but now even in the field of regulation that is based on public policy, it appears that States may allow transnational companies to make decisions about the

375 S. C. SYMEONIDES, *The American Choice-of-Law Revolution: Past, Present and Future*, cit.

regulatory reach of the state according to the information they have from their commercial operations, as it will happen under the Cloud Act's comity framework. Corporations then can have a say on whether the application of public policy would be beneficial or not on their own information on the possible effects of a conflict.

It is in this sense that data is different because it no longer serves the courts (but also the legislators) as a proxy for public policy – the regulation of a located thing according to the territory that it is located in makes sense insofar as the regulation of such thing serves in some way the interests of the state, such as the distribution of resources among the members of a located populace. But when the role of the state is providing the members of that populace access to the markets that distribute the profits generated from the processing of that thing, which in the context of data entails its continuous movement and global flow, the State's interest in regulating such thing is decoupled from the location of that thing, as there is no nexus left between the location of the thing and the benefits expected from its regulation.

Let us exemplify what is said here by reference to the provisions of the Cloud Act. Let us assume that the U.S. law maker has in its focus two competing interests (as I have argued above is indeed the case) namely securitization of private data flows and the facilitation of global market access for U.S. service providers. Data location is not a connecting factor conducive to the efficient protection of both these interests. According to §2703(h)(2)(A)(i), the comity-upon-motion option is conditional on the provider's reasonable belief that the target user is not a United States person *and* does not reside in the United States. Upon motion to quash, the court will ensure that this is the case before making a comity analysis. This provision effectively locates the focus of state interest in the close connection between the user and the state, rather than connection between the service (data storage) and the state. Data location, that suggests the latter type of connection, is not rejected completely as a valid ground for prescriptive jurisdiction, but can be overridden via comity analysis when the U.S. service provider risks "penalties"[376] due to the conflict of laws. This is in line with the state's facilitation interest. On the other hand, by foreclosing the comity analysis for disclosure orders regarding U.S. persons, the law basically provides for an effects jurisdiction rule with an irrefutable assumption that activity of U.S. persons and persons located in the U.S. will always be directed to the U.S, as the security interest of the state requires that procedural and substantive rights under foreign laws should not be invoked to limit the jurisdiction of American courts and lawmakers in cases where the effects of the activity is directed towards the U.S. It cannot be asserted that the law tries to uphold the jurisdiction of the natural judge of the user, as jurisdiction to issue a warrant in any case lies with the court of the judicial area in which the crime or activities related to the crime have occurred (Federal Rules of Criminal Procedure, Rule 41(b)(6)).

8. This paper sought to argue that the *comity-upon-request* framework provided in the new U.S. Cloud Act is a partly a result of the U.S. government's motivation to facilitate global market access of its domestic cloud computing service providers. To achieve this goal, an "information problem" as I have explained in this paper must be overcome, and I have argued that the comity analysis solution provided in the Cloud Act has been shaped to solve this information problem by shifting the job to determine and address conflicts of laws to the service providers. Through this

376 18 U.S.C. §2703(h)(3)(C).

authority, service providers now have a say in whether and when the exercise of extraterritorial prescriptive and enforcement jurisdiction is acceptable, a job that is traditionally within the exclusive competence of state organs, since it is typically considered to be a function of sovereignty.

My findings are dependent on two assumptions to be inferred properly. First, there must be an identifiable state interest of facilitating global market access, and this interest should be able to clash with other traditional state interests so that a novel jurisdictional rule that takes into account the information problem would be needed. Second, data location based territorial rules should be unable to meaningfully distribute authority between states in a way sensitive to the clashing state interests I have identified in my assessment of the first assumption. In this paper, I sought to provide evidence and observations to support these assumptions, and thus justify my inferences about the form of the new comity framework.

KAYAHAN CANTEKIN
European University Institute (EUI)