DOI 10.5817/MUJLT2016-2-4

AGAINST 'AGAINST DATA EXCEPTIONALISM'[*]

by

DAN JERKER B. SVANTESSON[**]

The April 2016 issue of the Stanford Law Review (Volume 68, Issue 4) contains an interesting article by Assistant Professor Andrew Keane Woods. In that article, titled 'Against Data Exceptionalism', Woods seeks to challenge the view that the nature of data is incompatible with existing territorial notions of jurisdiction. He argues that the nature of data is not unique, and that existing jurisdictional principles rooted in territoriality can be applied to data.

This is my response to his claims. I argue that Woods fails to refute 'data exceptionalism', and that his description of relevant jurisdictional issues is based on a misunderstanding leading to a conflation of different jurisdictional questions.

KEY WORDS

Data Exceptionalism, Territoriality, Jurisdiction, Data Privacy, Internet Law

1. INTRODUCTION

Some twenty years ago, we got to enjoy what arguably is the to-date most interesting academic sparring on the Internet law arena. I am of course referring to the fascinating exchange between Johnson and Post in one corner, and Goldsmith in the other. In their classic *Law And Borders - The Rise of Law in Cyberspace*, published in 1996 in the Stanford Law Review, Johnson and Post sought to illustrate that Cyberspace should be viewed as a separate 'space',[1] beyond the control of individual nations' regulation.

[*] The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

[**] nossetnavs@hotmail.com, Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Visiting Professor, Faculty of Law, Masaryk University (Czech Republic). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583).

[1] Johnson, D. R., Post, D. 1996. Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review,* vol. 48, no. 5, pp. 1367 - 1402.

Moreover, the article suggested that, to the extent that this separate space is to be regulated, such regulations would emerge in the form of self-regulation.[2] Goldsmith replied with his, equally classic, *Against Cyberanarchy* published in 1998 in the University of Chicago Law Review, arguing that

> *"Cyberspace transactions are no different from 'real-space' transnational transactions.* […] *There is no general normative argument that supports the immunization of cyberspace activities from territorial regulation."*[3]

This was followed by Post's perhaps somewhat less noticed, but equally engaging, article *Against 'Against Cyberanarchy'* published in 2002 in Berkeley Technology Law Journal.[4]

The core issues debated then remain relevant today, and Goldsmith's influence is clear on the arguments Woods now presents in his recent article *Against Data Exceptionalism*[5] published in Stanford Law Review. Indeed, Woods was presumably inspired by Goldsmith's choice of title. Since my aim with this note is to refute some of Woods' key claims, I thought it appropriate to similarly draw inspiration from Post's choice of title.

Yet, it is not just the respective choices of titles that the discussion below has in common with the famous academic exchange mentioned above. Like Goldsmith, Woods is committed to the territoriality principle, and like the cyberlibertarians I (like many other recent commentators) consider that the territoriality thinking fails us in the online context. At the same time, as Woods correctly notes, the discussion to be had now is somewhat different to the debates that go before it. Speaking about the exchange between Johnson and Post on the one hand and Goldsmith on the other, he points out that:

> *"That scholarship was largely about spillovers: behavior in one state spilling over into another state via the Internet. The jurisdictional question in such*

---

2 *Id.* at 1367.

3 Goldsmith, J. L. 1998. Against Cyberanarchy, *The University of Chicago Law Review,* vol. 65, no. 4, pp. 1199-1250.

4 Post, D. 2002. Against 'Against Cyberanarchy', *Berkeley Technology Law Journal,* vol. 17, no. 4, pp. 1365-1388.

5 Woods, A. K. 2016. Against Data Exceptionalism, *Stanford Law Review,* vol. 68, no. 4, pp. 729-790.

> *a case is whether a nation may "apply its law to extraterritorial behavior with substantial local effects".*"[6]

In contrast, Woods' article and this response are concerned with

> *"how a nation can apply its laws to local behavior with local effects when the data related to the act happens to be stored in the global cloud."*[7]

Nevertheless, 'exceptionalism' and territoriality occupy centre stage now as they did then.

The stated aim of Woods' article is to challenge the view that the nature of data is incompatible with existing territorial notions of jurisdiction.[8] To achieve this, he seeks to illustrate that the nature of data is not unique (his Part II), and that existing jurisdictional principles rooted in territoriality can be applied to data (his Part III). It is those two parts of his article I focus on, and here I do not seek to comment on his problem and context description (his Part I) or his observations as to transnational conflicts of laws and proposals for how the *Electronic Communications Privacy Act* should be reformed (his Parts IV and V).

2. MY PERSPECTIVE AND HOW IT CLASHES WITH WOODS'

Woods explains to us that:

> *"Despite the technological wizardry of modern life, the "cloud" is actually a network of storage drives bolted to a particular territory […]. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries. These precedents suggest numerous grounds for states to assert jurisdiction over data."*[9]

For some time now, I have – without seeking my arguments in wizardry or mysticism – argued that strict territoriality is ill-equipped for today's modern society characterised by constant, fluid and substantial cross-border

---

6 *Id.* at 738 (footnotes omitted).
7 *Id.* at 738.
8 *Id.* at 729.
9 *Id.* at 719.

interaction, not least via the Internet. This places me in the same boat, or at least in the same flotilla, as the scholars, practitioners and Internet companies Woods claims to prove wrong in his article.

In an article published in the *American Journal of International Law Unbound* in 2015, I advanced a proposal for a new jurisprudential framework for jurisdiction that is not based on the territoriality principle:

> *"In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:*
> *(1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction;*
> *(2) the State seeking to exercise jurisdiction has a legitimate interest in the matter; and*
> *(3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests."*[10]

I take the view that the territoriality thinking that is characteristic of the current paradigm is inadequate in many areas such as e.g. human rights law, environmental law, and anti-trust law; that is, the problems that come to the fore when applying a territoriality thinking to the online environment is merely yet another example of why territoriality fails as a foundational core principle for jurisdiction in our modern world. Thus, my proposal does not depend on data exceptionalism as such. Nevertheless, I present a distinctly territoriality-nihilistic view that clashes with Woods' assertion that

> *"the data exceptionalists are wrong to suggest that the cloud changes anything fundamental as a matter of prescriptive jurisdiction or enforcement jurisdiction; the same old (territorial) rules apply to this new Internet technology."*[11]

In other words, as my claim gains strength from data exceptionalism, if Woods is right, that undermines my claim.

---

[10] Svantesson, D. J. B. 2015. A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft: Comment on "A New Jurisprudential Framework for Jurisdiction", *American Journal of International Law Unbound*, vol. 109, pp. 69-74.

[11] Woods, *supra note* 5 at 765.

3. LACKING SHARPNESS OF FOCUS

Before moving into the substance, it should be noted that it is not always easy to understand what Woods actually is committing to in his arguments. For example, he variously claims that *"data is not as novel as the data exceptionalists suggest"*[12], and that *"data is not conceptually exceptional"*.[13] Of course, under the first claim, he is not disputing the novelty as such, he just asserts that some people may have overstated the degree of novelty. In the second claim, he asserts that the relevant features are, in a binary sense, not exceptional. It would have been better had he committed to one view and stuck with it.

More importantly, despite the article's title being "Against Data Exceptionalism" Woods, does not actually do much to oppose data exceptionalism as such. Rather what Woods is in fact opposing – while he stubbornly sticks to the misguided label of "data exceptionalism" – is "cloud data exceptionalism", and indeed on some occasions "cloud exceptionalism"[14]. As he himself expressly acknowledges:

> *"To be clear, these claims are not solely about the nature of data, but rather about the role of data in the cloud."*[15]

The distinction between *data exceptionalism* on the one hand, and *cloud data exceptionalism* on the other, is not merely a stylistic matter. For example, even if Woods would have refuted the claim of cloud data exceptionalism – and I do not think he has done so – it would remain possible to argue for data exceptionalism.

4. WOODS FAILS TO REFUTE "DATA EXCEPTIONALISM"

To prove that cloud data lacks a novelty that would support the data exceptionalist view, Woods takes the reader on a laborious journey involving the exercises of mapping out what features could make cloud data unique, and why in fact these features do not make such data unique.

The features Woods attribute to cloud data are (1) intangibility, (2) mobility, (3) divisibility and fungibility and (4) the distance between

---

[12] *Id.* at 763.

[13] *Id.* at 764.

[14] "the jurisdictional challenges presented by the global cloud are not conceptually as novel as they seem." *Id.* at 729.

[15] *Id.* at 755.

the asset holder and the asset. It is not clear why he opted for these particular features, at the expense of other relevant features such as the fact that data can relate to several persons at the same time thereby creating simultaneous jurisdictional links to multiple states. Either way, since courts can choose to treat data as either an intangible or tangible asset, Woods also analyses data as a tangible asset.

For each of the mentioned features, Woods shows that they are not unique. For example, in showing that intangibility is not on its own a novel feature, he points to the fact that courts have adjudicated disputes over intangible assets like stock and debts for many years. Similarly, to show that mobility as a feature of an asset class is not unique to data, Woods stresses that money can be wired from one location to another in an instant.

His approach is, however, misguided both in relation to each individual component it addresses and as a whole. For example, under a heading suggesting a discussion of the fact that data are 'divisible' and 'fungible', Woods embarks on an elaborate discussion of how users do not care whether their content, as presented by cloud companies, is represented by the "same" ones and zeros as they themselves upload.[16] This is of course not of any interest whatsoever, and Woods would have done better ignoring such imaginary issues and instead paying attention to real problems such as the difficulty of attributing a location to data that exists in fragments on multiple servers rather than as a whole on any one server.

Further, in showing the lacking uniqueness of intangibility, Woods enthusiastically points to how:

> *"courts have come up with a number of different approaches to locating intangible assets. For example, intellectual property rights like trademarks are typically found to be located wherever they were created or registered. Debts are typically located where the debtor resides—as that is typically, though not always, where steps can be taken to ameliorate the debt."*[17]

However, he does nothing to consider whether any of these methods would actually work in relation to data. Would it, for example, be appropriate to locate data wherever they were created (data not being 'registered' removes one of the mentioned ground automatically)? Or can

[16] *Id.* at 759-760.
[17] *Id.* at 756-757.

data be located to where the 'data subject' resides? The point is that unless the solutions advanced in relation to other intangibles may prove to be of use also for data, Woods' exercise tells us very little of interest.

Furthermore, as to money – the type of intangible he relies on the most – he seems to completely overlook the fact that money in its modern form is in fact also data – it is because money is data that it can be 'wired' from one side of the planet to another. Thus, no aspect of money can be used to argue that data is not unique since all he is doing is arguing that data is not unique as data (in the form of money) unsurprisingly shares the characteristics of data.

The most serious flaw in Woods' approach here is, however, his failure to consider, in a cumulative manner, the features he discusses; that is even if he manages to find similarities in relation to each of the features he discusses, unless he finds some intangible that shares *all* of those features, the uniqueness of cloud data has clearly not been refuted. It is simply remarkable that he makes the claim that

> *"None of the features that are thought to make data novel are in fact novel—whether the features are considered individually or as a whole,"*[18]

when in fact he has only discussed the features individually, not as a whole.

5. WOODS AND POSSIBLE GROUNDS FOR JURISDICTION

The part of Wood's article in which he seeks to convince the reader that all is well in the application of existing jurisdictional principles to the setting of cloud data opens with a telling, and rather terrifying, claim:

> *"Jurisdiction is and likely always will be rooted in territoriality. States are the sovereigns of their territory and their citizens. Accordingly, they can regulate acts taking place on their soil as well as acts that affect their citizens, regardless of the location of those acts. This means that a state might legitimately assert its jurisdiction over a piece of data because that data or its controller is located in the state's territory, or simply because the data is needed for law enforcement there, regardless of where the data is stored or where the company is headquartered."*[19]

[18] *Id.* at 763 (emphasis added).
[19] *Id.* at 764 (footnote omitted).

I say terrifying as it would be worrying indeed if any state could demand access to any piece of data it wanted, anywhere in the world, simply because the data is needed for law enforcement there, for example in order to pursue human rights advocates, political dissidents and others perceived as undesirables by that state.

The telling part of the quote is that it reveals a deep misunderstanding of jurisdiction in the sense of a conflation of two separate matters. Under orthodox thinking, states can indeed regulate *acts* taking place on their soil as well as *acts* that affect their citizens, regardless of the location of those acts. However, that does not tell us anything about jurisdiction *over a piece of data* that is stored outside the state by a company with no link to that state. The first is a matter of jurisdiction over the offense, the other a matter of jurisdiction over the data that e.g. may be used as evidence in relation to that offense.

At any rate, the fact that grounds for jurisdiction can be found, or indeed imagined, says nothing about their suitability, and it does not bring Woods any further on his quest against cloud data exceptionalism. Rather here, again in a Don Quixote like fashion, Woods vigorously engages with imaginary opponents, while staying well clear of the many real obstacles to the claims he makes. As noted by Clopton in his interesting response to Woods' article:

> *"[T]he most telling statement in Woods's excellent article comes early on: "Showing that the jurisdictional challenges presented by the global cloud are not conceptually novel does not resolve those problems…" Data may not be exceptional, and the legal puzzles posed by data sound in existing notions of jurisdiction and conflict of laws. The problem, however, is that existing answers to these puzzles are unsatisfying. They are unsatisfying in that they do not provide clear answers, but instead pose even more challenging normative questions. And they are unsatisfying because some consensus answers sit on shaky normative footing."*[20]

It is quite simply impossible to imagine any situation in relation to which it is not possible to imagine a jurisdictional rule as long as one is freed from the responsibility of finding a jurisdictional rule that actually works well for that situation. Thus, for example, in stating that we can base

[20] Clopton, Z. D. 2016. Data Institutionalism: A Reply to Andrew Woods, *Stanford Law Review Online*, vol. 69, pp. 1-9 (footnote omitted).

jurisdiction on the location of data,[21] Woods blissfully ignores the difficulty of how we address situations where a decision about jurisdiction must be made by a party (e.g. a law enforcement agency) that is not able to ascertain the location of the data, at the time the decision as to jurisdiction must be made.

Furthermore, in Woods' discussion of jurisdiction based on the location of the harm,[22] we again see worrying signs of confusion resulting in conflation. Here he claims that:

> *"States have a considerable interest in ensuring that their laws are enforced. For this reason, one sound basis for jurisdiction would be to say that the state where the crime occurred has a compelling interest in gaining access to digital evidence necessary to enforce its laws."*[23]

Having provided an example of Scotland Yard investigating a string of bank robberies in London, in relation to which critical evidence likely resides on one of the suspect's Dropbox accounts, Woods concludes that:

> *"No one doubts that the U.K. Parliament has the legislative jurisdiction to pass a law criminalizing bank robbery. Indeed, it has a rock-solid jurisdictional basis for doing so—namely, controlling the activities that occur on its soil."*[24]

Here he is, however, no longer talking about jurisdiction over the data but rather jurisdiction over the criminal matter as such. Indeed, he admits this by going on to note that:

> *"Getting access to digital evidence related to a U.K. crime—evidence that may or may not be in the United Kingdom's territory—is a question of enforcement jurisdiction, which will be discussed in more detail below."*[25]

Thus, in the end, the disappointing conclusion must be that all Woods is saying about prescriptive jurisdiction is actually irrelevant for the topic ofJhis article which is instead focused on enforcement jurisdiction – or as I

---

[21] Woods, *supra note* 5 at 766-767.
[22] *Id.* at 767-768.
[23] *Id.* at 767.
[24] *Id.* at 767-768.
[25] *Id.* at 768.

have argued elsewhere, "investigative jurisdiction"[26] – in the form of getting access to digital evidence.

Unfortunately, no compensation for this disappointment is found in Woods' treatment of enforcement jurisdiction. Here he merely echoes conventional claims such as that states can exercise enforcement jurisdiction only against persons or entities with either a presence or with assets within that state's territory.[27] This brings us no closer to solutions, and indeed, it does little for Woods' crusade against cloud data exceptionalism.

Finally, in this context, to understand Woods' willingness, or indeed eagerness, to embrace sub-standard grounds for jurisdiction with obvious practical flaws, we must understand his point of departure which is found in a legitimate, albeit unhelpfully one-dimensional, concern about law enforcement efficiency, as well as in misguided conceptions as to the necessary consequences of data exceptionalism.

Starting with the latter of these concerns, we can note how Woods asserts that

> *"if data is not as different as many have suggested, then states need not commit to narrowly defining their authority over data based on a single test, such as the location of the data or the domicile of the company."*[28]

However, it is not clear why data exceptionalism would force us to commit to narrowly defining authority over data based on a single test. Equally surprisingly, Woods assumes that data exceptionalists are those who *"argue that data challenges territorial conceptions of sovereignty and therefore cries out for a global treaty"*[29] (emphasis added). Obviously, data exceptionalists may also promote the option of a global treaty. However, they but need not do so. To conclude, data exceptionalism may not necessitate all that Woods suggests it does.

Discussing a hypothetical scenario in which an Indian woman is murdered in India, with the primary suspect being an Indian man, and the only link outside India being that the Indian police wishes to get

---

[26] Svantesson, D. J. B. 2014. The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses, *Stanford Journal of International* Law, vol. 50, no. 1, pp. 53-102.

[27] Woods, *supra note* 5 at 769-770.

[28] *Id.* at 735.

[29] *Id.* at 788.

access to the suspects Google account, Woods complains that it is "unfair" that

> *"the Indian law enforcement agent must ask an American judge to sign off on her request to receive access to the data, despite the fact that an Indian magistrate has already deemed the data crucial to the investigation."*[30]

It is easy to sympathise with Woods' concern. However, if we, in the example, replace all references to 'India' with 'North Korea', and we change the crime from 'murder' to 'political dissent', the picture changes. Thus, the 'North Korea test' illustrates that the perceived unfairness in Woods' example only holds in relation to (a) certain crimes, and (b) certain countries.[31] This severely undermines the correctness of his perception of the ills that will flow from an acceptance of data exceptionalism.

6. FINAL REMARKS

Given the above, Woods' attack on cloud data exceptionalism, and his accompanied defence of territoriality, fizzles out into nothingness. His perhaps most important claim that

> *"in many ways, it is easier for courts to assert jurisdiction over data than over intangible assets because, unlike debts or stock, data has a physical and therefore territorial presence wherever it is stored"*[32]

quite simply ignores too large parts of reality to be afforded general applicability. First, a theoretical location helps little when at the time a jurisdictional decision is made that location is practically unascertainable. Second, as the location of data can be so easily manipulated, the wisdom of attaching significance to the location of data is questionable. Thus, in my assessment, Woods – despite his bold claims – have neither refuted cloud data exceptionalism nor data exceptionalism. And it remains my view that the difficulty of determining the location of data, and especially of cloud

---

[30] *Id.* at 745-746.

[31] Woods would presumably agree with this given some of his other writings (see e.g.: Jennifer Daskal and Andrew Keane Woods, *Cross-Border Data Requests*: A Proposed Framework, Lawfare November 24, 2015 https://lawfareblog.com/cross-border-data-requests-proposed-framework).

[32] Woods, *supra note* 5 at 761.

data, undermines the prevalent territoriality thinking. As noted by Post in Against 'Against Cyberanarchy',

> *"Settled law, and received principles, are worthy of respect; but at times they need to be reconsidered. This is one of those times."*[33]

This remains true today.

LIST OF REFERENCES

Clopton, Z. D. 2016. Data Institutionalism: A Reply to Andrew Woods, *Stanford Law Review Online*, vol. 69, pp. 1-9.

Daskal, J., Woods, A. K. *Cross-Border Data Requests: A Proposed Framework*, Lawfare November 24, 2015. Available from: https://lawfareblog.com/cross-border-data-requests-proposed-framework.

Goldsmith, J. L. 1998. Against Cyberanarchy, *The University of Chicago Law Review,* vol. 65, no. 4, pp. 1199-1250.

Johnson, D. R., Post, D. 1996. Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review*, vol. 48, no. 5, pp. 1367-1402.

Post, D. 2002. Against 'Against Cyberanarchy', *Berkeley Technology Law Journal*, vol. 17, no. 4, pp. 1365-1388.

Svantesson, D. J. B. 2014. The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses, *Stanford Journal of International Law*, vol. 50, no. 1, pp. 53-102.

Svantesson, D. J. B. 2015. A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft: Comment on "A New Jurisprudential Framework for Jurisdiction", *American Journal of International Law Unbound,* vol. 109, pp. 69-74.

Woods A. K. 2016. Against Data Exceptionalism, *Stanford Law Review,* vol. 68, no. 4, pp. 729-790.

[33] Post, *supra note* 4 at 1387.