2015

Data Nationalism and Its Discontents

Christopher Kuner

DATA NATIONALISM AND ITS DISCONTENTS

Christopher Kuner[*]

INTRODUCTION

Data localization or data nationalism, which terms I will use synonymously here, has received growing attention. Numerous commentators (including myself)[1] have raised questions about efforts at the national or regional level to regulate the flow of data across borders or to create incentives to localize data processing and storage.[2] This is the topic of the important new article *Data Nationalism* by Anupam Chander and Uyê P. Lê published in the *Emory Law Journal*.[3]

Chander and Lê provide a thoughtful and useful analysis of regulatory initiatives that promote data nationalism. They have cast their net widely to include examples from around the world (including citation of materials in languages such as Russian and Vietnamese). The Article's careful consideration of numerous data localization initiatives, the motivations behind them, and their social, economic, and legal implications fills an important need in the literature on Internet regulation.

In this short piece I will both respond to the Article and comment on some important overarching issues that it raises. My comments are based on a draft of September 8, 2014 with which I have been provided and which I have not been able to check against the final published text (though references to the final version have been inserted).

---

[*] Co-Director, Brussels Privacy Hub, Vrije Universiteit Brussel (VUB); Associate Professor of Law, University of Copenhagen; Affiliated Lecturer, University of Cambridge; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels.

[1] *E.g.*, Christopher Kuner, *Requiring Local Storage of Internet Data Will Not Protect Privacy*, OUPBLOG (Dec. 6, 2013), http://blog.oup.com/2013/12/data-security-privacy-storage-law/.

[2] *See, e.g.*, DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., FALSE PROMISE OF DATA NATIONALISM (2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf; W. Kuan Hon et al., *Policy, Legal and Regulatory Implications of a Europe-only Cloud* (Queen Mary Univ. of London, Sch. of Law, Legal Studies Research Paper No. 191/2015, 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2527951; Judith Rauhofer & Caspar Bowden, *Protecting their own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* (Univ. of Edinburgh Sch. of Law, Research Paper Series No. 2013/28, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2283175.

[3] 64 EMORY L.J. 677 (2015).

The authors provide detailed analysis of current data localization initiatives, focusing on their internal contradictions and why they are unlikely to meet their intended aims. I share their concern about many of these initiatives and am skeptical that many of them will result in better protection of individual rights or increased Internet security. At the same time, I take issue with a few of the authors' arguments and think that their case would have been stronger had they addressed three points in greater detail.

First of all, the types of measures examined in the Article are in fact not new and have existed since the 1970s. The fact that they seem to be increasing in number over the last few years has as much to do with increasing public unease with globalization and a desire to maintain national borders on the Internet, as with protectionism.

My second point concerns the authors' definition of "data nationalism." I believe that they have tarred with the same brush initiatives that have very different motivations, and in particular have attributed protectionist motives to some measures seeking to protect constitutional and human rights on the Internet.

My third point is that the authors could have put forward a stronger normative basis for their criticisms. Without this, it will be difficult to counteract current moves towards data nationalism.

I. HISTORICAL ROOTS OF DATA NATIONALISM

Approximately the first half of the Article is devoted to an overview of data localization measures around the world. The majority of those discussed date from 2010 or later,[4] with a few exceptions.[5] The authors write that these initiatives are generally motivated by concerns about widespread electronic spying by U.S. intelligence agencies (i.e., the Snowden revelations), efforts to promote domestic economic development, the protection of privacy and security, and the furtherance of domestic law enforcement interests.

---

[4] *See id.* at 686–88, 690–92, 701–02, 704–06 (discussing measures taken in 2011 by the People's Bank of China to require data to be stored in China; initiatives announced in February 2013 by the French Minister of Industry to localize data processing in France; legislation introduced in 2013 in Russia; and legislation in Vietnam to control speech on the Internet dating from 2013).

[5] For example, the E.U. Data Protection Directive 95/46, which came into force in 1998, and privacy legislation introduced in British Columbia in 1996. Chander & Lê, *supra* note 3, at 685–86, 688.

In fact, the phenomena that the authors describe date back to the years when international computer networks began to become widely used, i.e., to the 1970s and 1980s. For example, in 1976 Brazil required the prior permission of a government board for the use of international computer networks (such as corporate networks and foreign databanks) that transferred or accessed data outside the country.[6] Around the same time, government officials and commentators in countries such as Canada,[7] France,[8] and Sweden[9] also expressed concerns about uncontrolled transborder flows of personal data. Thus, the "Internet border controls" that the authors refer to as being a relatively new phenomenon are actually decades old, at least with regard to closed electronic networks.[10]

I have referred elsewhere to the interest that these initiatives seek to protect as "informational sovereignty,"[11] a concept that arose because of widespread unease with the breakdown of national regulatory borders caused by electronic data flows. The arguments for and against extending such boundaries to the Internet are reflected in the debate from the late 1990s and early 2000s between David Post and Jack Goldsmith.[12] From the phenomena that the authors cite, it seems that Goldsmith's view of Internet regulation (i.e., that it is

---

[6] *See* HANS-JOACHIM MENGEL, INTERNATIONALE ORGANISATIONEN UND TRANSNATIONALER DATENSCHUTZ [INTERNATIONAL ORGANIZATIONS AND TRANSNATIONAL DATA PROTECTION] 201 (1984).

[7] *See, e.g.*, Allan Gotlieb, Charles Dalfen & Kenneth Katz, *The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles*, 68 AM. J. INT'L L. 227, 246–47 (1974).

[8] *See* John M. Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers?*, 10 LAW & POL'Y INT'L BUS. 1055, 1065–66 (1978). Eger quoted French Justice Ministry official Louis Joinet, who noted,

> Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows.

Id. at 1065–66 (quoting Statement of Louis Joinet, French Magistrate of Justice, Remarks before the Organization for Economic Cooperation and Development Symposium on Transborder Data Flows and the Protection of Privacy, in Vienna, Austria (Sept. 1977)).

[9] *See, e.g.*, G. Russell Pipe, *National Policies, International Debates*, J. COMM., Summer 1979, at 114, 121 (quoting a member of the Swedish parliament saying the risks inherent in the storage of data outside the country means that "the critical mass of data concerning the Swedish economy and its citizens should never leave the national territory" (internal quotation marks omitted)).

[10] Chandler & Lê, *supra* note 3, at 679.

[11] *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 28–31 (2013).

[12] *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); David G. Post, *Against* Against Cyberanarchy, 17 BERKELEY TECH. L.J. 1365 (2002).

both natural and appropriate for governments to extend their regulatory reach to cyberspace) has been gaining the upper hand in recent years.

The transfer of national borders to the online space reflects society's ambivalence about the benefits and drawbacks of globalization: on the one hand we have grown accustomed to the global availability of goods and services, but on the other hand we are unsettled by the breakdown of barriers that seems to threaten our national and regional identities. The Snowden revelations and other recent developments have increased the pace and intensity of these anxieties, but the deep-seated nature of these concerns shows the importance of developing an underlying normative framework to address them.

II. DISTINGUISHING RIGHTS PROTECTION FROM PROTECTIONISM

Phenomena such as intelligence surveillance, the globalization of the information economy, and privacy violations by Internet companies have led to initiatives to strengthen constitutional and fundamental rights online. E.U. data protection law is particularly relevant as an example in this regard, as dozens of countries around the world use it as a model.

The potential to misuse data protection law as a vehicle to further domestic business interests certainly exists; the Article mentions examples of this from France and Germany.[13] However, E.U. data protection law is based on constitutional provisions of the Treaty of Lisbon, which grants individuals a right to data protection[14] and gives legal effect to the Charter of Fundamental Rights of the European Union.[15] Restrictions on transborder data flows are a part of E.U. data protection law,[16] as demonstrated by the recent reference to the Court of Justice of the European Union (CJEU) in the case *Schrems v. Data Protection Commissioner*.[17] That case involves the question of whether the European Commission's adequacy decision creating the E.U.–U.S. Safe

---

[13] Chander & Lê, *supra* note 3, at 690–94.

[14] Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47, 55 [hereinafter TFEU].

[15] TFEU art. 6; *see also* Charter of Fundamental Rights of the European Union art. 8, Mar. 30, 2010, 2010 O.J. (C 83) 389, 393 (granting a right to data protection) [hereinafter E.U. Charter of Fundamental Rights].

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, arts. 25–26, 1995 O.J. (L 281) 31, 33 [hereinafter Council Directive].

[17] *Reference for a Preliminary Ruling from High Court of Ireland (Ireland) made on 25 July 2014 — Maximillian Schrems v Data Protection Commissioner (Case C-362/14)*, 2014 O.J. (C 351) 5.

Harbor should be reevaluated in light of widespread access to data by U.S. law enforcement, and whether the Member State data protection authorities should be allowed to determine whether the Safe Harbor provides adequate protection under the Lisbon framework.[18]

Differences in privacy protection and the understanding of fundamental rights between the European Union and the United States may cause some in the United States to regard European Union legal restrictions on data flows, and other European concerns about the data processing practices of U.S. companies, as protectionist; indeed, President Obama seems to take this position.[19] However, a review of the historical record concerning the evolution of data flow restrictions in E.U. data protection law indicates that they are based more on policy considerations, such as avoiding circumvention of the law and guarding against specific data processing risks in other countries, than on protectionism.[20]

In the European Union the protection of privacy is supplemented by the concept of data protection, which regulates the processing of data that can be used to identify an individual person regardless of whether such data are inherently personal or private.[21] The Article does not distinguish between the two concepts and often deals with data security (i.e., I.T. security) when it purports to discuss privacy. In E.U. data protection law, data security is an integral part of privacy protection but is just one of many requirements for data processing.[22] It would have been better if the authors had interpreted the term "privacy" to include other issues dealing with the regulation of data processing in a broader sense. They also criticize public sector data localization initiatives in Europe (e.g., in some Scandinavian countries), without considering whether

---

[18] *Id.*

[19] *See* Murad Ahmed, *Obama Attacks Europe over Technology Protectionism*, FIN. TIMES, Feb. 16, 2015, http://www.ft.com/intl/cms/s/0/41d968d6-b5d2-11e4-b58d-00144feab7de.html (quoting the President as stating with regard to European resistance to the business practices of U.S. technology companies, "oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests" (internal quotation mark omitted)).

[20] See KUNER, *supra* note 11, at 101–20, for an analysis of the policies underlying restrictions on transborder data flows under E.U. data protection law.

[21] For example, the E.U. Charter of Fundamental Rights contains separate articles dealing with data protection, *see* E.U. Charter of Fundamental Rights art. 8, and respect for private and family life, *see id.* art. 7.

[22] See, for example, the E.U. Data Protection Directive 95/46 that contains many other obligations, such as Article 7 (requiring that there be a legal basis for the processing of personal data), Article 8 (setting conditions for the processing of so-called "sensitive data"), Articles 10 and 11 (requiring that information about data processing be provided to data subjects), and Article 12 (granting data subjects a right of access to their data). Council Directive, *supra* note 16, at 40–42.

there cannot be legitimate reasons for setting a higher standard for data transfers by public authorities, since they have responsibilities to the community that do not apply to private actors.

While the authors do imply that governments have a legitimate interest in protecting individuals online,[23] they neglect to examine some legal questions that are crucial to define the scope of this interest. For example, since enforcement jurisdiction is primarily territorial, may the location of assets or equipment in the jurisdiction be justified as a way to make it easier to enforce local law? Can data nationalism really bring any protection against the enforcement of foreign legal norms?[24] Does the fact that under Article 13 of the European Convention on Human Rights individuals must be provided with "an effective remedy before a *national* authority" mean that it must be possible for them to assert their rights before a court or regulatory authority in their own country?[25] And wouldn't the motivations for data nationalism diminish if the countries of the world could agree on an international legal framework for issues such as Internet jurisdiction and online privacy (unlikely as this is)?

The Article makes a strong case against using data access by foreign intelligence services as justification for data localization measures: since much data sharing seems to be carried out between different intelligence services around the world, in the end data nationalism may only facilitate access by local intelligence services. While this is a valuable point, it begs the question of whether a society may not legitimately be more concerned about access by foreign intelligence services, since they are not subject to democratic control by the country being surveilled. Moreover, a country may view foreign surveillance as an act of spying, which raises a separate set of issues.

The authors also fail to mention the market pressures that contribute to the current increase of data localization measures. Based on my personal experience, and discussions with many companies and lawyers over the last few years, there is a trend for European companies to refuse to deal with companies in other regions (particularly in the United States) that do not

---

[23] Chander & Lê, *supra* note 3, at 718–21.

[24] This last point has received increased attention because the United States Court of Appeals for the Second Circuit is hearing a case that concerns whether Microsoft can be compelled by a U.S. warrant to produce emails stored at its data center in Ireland. *See* Brief for Appellant at 5, 12–13, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-cv (2d Cir. Dec. 15, 2014).

[25] Convention for the Protection of Human Rights and Fundamental Freedoms art. 13, *opened for signature* Nov. 4, 1950, C.E.T.S. No. 005 (entered into force Sept. 3, 1953) (emphasis added).

implement strict E.U. standards for the processing of personal data; this can be seen, for example, in an unwillingness to accept the Safe Harbor as a legal basis for data transfers to the United States. A number of U.S. Internet companies have set up local data processing centers as a way to counter these pressures and gain more business.[26] There is thus a kind of "chicken or egg" question that needs to be addressed with regard to data localization measures, i.e., did governments initiate them to benefit domestic interests, or was it domestic pressures from business and individuals that led to governments becoming interested in the topic?

III. DATA NATIONALISM AND NORMATIVE VALUES

Many of the authors' points concern the harmful effect of data localization on the ability to deliver Internet services in a seamless and cost-efficient fashion. For example, they note that data nationalism "poses a mortal threat to the new kind of international trade made possible by the Internet—information services such as those supplied by Bangalore or Silicon Valley."[27] I am reminded here of the famous review of Posner's *Economic Analysis of Law* by Leff, who points out that using economic efficiency as the measure of legal rules requires an initial assumption that it is inherently desirable and should be given preference over other values.[28] Likewise, the authors criticize the economic effects of data nationalism but do not address the central question that these arguments raise: what if a country has decided that it wants to sacrifice a certain amount of economic efficiency in exchange for promoting other legitimate values that it believes are furthered by data nationalism?

The lack of a strong set of normative principles for criticizing data nationalism leads the authors to rely too much on factual arguments that ultimately depend on one's point of view. For example, they criticize data nationalism as undermining data security by increasing the incentives for choosing local companies with weak security measures to process data, instead of larger global companies that are better able to provide strong security.[29] But one could argue that hackers and national intelligence services tend to target

---

[26] *See, e.g.*, Murad Ahmed, *Business Fears over US Spying Prompt Amazon to Offer Web Hosting in Europe*, FIN. TIMES, Oct. 24, 2014, at 15, *available at* http://www.ft.com/intl/cms/s/0/56181a6e-5a96-11e4-b449-00144feab7de.html.

[27] Chander & Lê, *supra* note 3, at 681.

[28] Arthur Allen Leff, *Economic Analysis of the Law: Some Realism About Nominalism*, 60 VA. L. REV. 451, 464–65 (1974) (reviewing RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (1973)).

[29] Chander & Lê, *supra* note 3, at 716–17.

large global data centers because they have more data to access, thus putting them more at risk; the authors even admit this, calling it the "Jackpot" problem. They also state that data localization requires information service providers to build out a physical infrastructure in every jurisdiction where they operate, thereby increasing costs and making it impossible to render many online services on a global basis.[30] However, shortly afterwards they admit that there are many varieties of data localization and that while some explicitly require the use of domestic servers to process data, others are less visible and more indirect.[31]

Data nationalism also creates new risks that are not mentioned in the Article. As countries increasingly apply their national law to cross-border activities on the Internet, it is inevitable that it will become increasingly necessary to "tag" or otherwise mark data to indicate the country whose law applies to its processing.[32] This process will likely require the generation of further datasets to identify the data being processed, which can itself increase privacy risks.

I would have liked to see a more detailed examination of the underlying values of democracy and legality that are threatened by data nationalism. For instance, the Universal Declaration of Human Rights of 1948 (UDHR) and the International Covenant on Civil and Political Rights of 1966 (ICCPR) both protect the freedom to transfer data "regardless of frontiers."[33] The Article briefly mentions the right to borderless communication under the ICCPR, but more discussion of the status of this right in the Internet age could have been included, as well as an explanation of its value in relation to other interests and rights that governments often use as a basis for enacting data localization measures. The authors also could have mentioned that this same right to communicate regardless of frontiers is affirmed by the E.U.'s Charter of Fundamental Rights (Article 11), and could have referred to the work done with regard to online surveillance by the Office of the U.N. High Commissioner for Human Rights.[34]

---

[30] Chander & Lê, *supra* note 3, at 723–24, 729.

[31] *Id.* at 727.

[32] *See* Paula J. Bruening & K. Krasnow Waterman, *Data Tagging for New Information Governance Models*, IEEE SECURITY & PRIVACY, Sept.–Oct. 2010, at 64 (discussing data tagging).

[33] *See* Universal Declaration on Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/Res/217(III), art. 19 (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 19(2), *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 14668 (entered into force Mar. 23, 1976).

[34] *See Right to Privacy in the Digital Age*, U.N. OFFICE OF THE HIGH COMM'R FOR HUM. RITS., http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (last visited Mar. 2, 2015).

In sum, I think that the authors need to make a better case regarding the normative values supporting a criticism of data nationalism. A number of them come to mind, such as freedom of expression, antidiscrimination, privacy as a fundamental right, and ethical considerations. A useful starting point in this regard is the opinion of the European Data Protection Supervisor (EDPS) on Internet governance of June 23, 2014, which both takes a strong stand against data nationalism and emphasizes that an open and free Internet can best be achieved by affirming commonly shared international rights and values.[35]

CONCLUSIONS

Chander and Lê have produced a valuable piece of scholarship that can serve as a starting point for serious discussion of data nationalism. As an internationalist who abhors nationalism in any form, whether it concerns data or anything else, I share many of their views. To the extent that the phenomena described in the article reflect parochial or protectionist tendencies, they threaten our freedoms and should be resisted.

At the same time, I feel it is important to point out that restrictions on data transfers may reflect different constitutional values in other legal systems that cannot simply be brushed aside as "protectionist." This is essential in order to distinguish between actual protectionism and measures that simply reflect the divergent values of different legal systems. While the authors do discuss the social consequences of data nationalism, such as its potential for restricting freedom of expression, these points seem outweighed by their emphasis on economic considerations. The roots of data nationalism are often based on more than mere protectionism.

The distinction between rights protection and protectionism can often be in the eye of the beholder, and it is thus difficult to differentiate the constitutional and legal issues raised by restricting data flows from the hidden economic agendas that may be at play. This raises the issue of whether the definition of data nationalism should be based on an objective or a subjective standard. For instance, is an initiative to protect privacy rights online to be classified as "protectionist" because it has the effect of restricting data flows, even if this was not its primary purpose? Or is there some element of intent required when

---

[35] *Opinion of the European Data Protection Supervisor on the Commission Communication on Internet Policy and Governance—Europe's Role in Shaping the Future of Internet Governance*, at para. 12 (June 23, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-06-23_Internet_Governance_EN.pdf.

classifying an initiative as protectionist? Governments must be much more honest in explaining the motivations behind data localization initiatives. Clothing industrial policy in the language of legality can corrode public trust in the status of fundamental values as standing apart from partisan interests.

In order to combat data nationalism, it is necessary to articulate a positive case in favor of a free and borderless Internet. This means that it is important to concentrate as much on the virtues of allowing data to flow freely as on the faults of data localization, and to base the argument on fundamental values and not just on economic and practical considerations. This can only be done by placing oneself in the mental shoes of those in other legal systems and developing arguments that resonate on a global level. We also require a detailed investigation of the implications of data nationalism for values such as freedom of expression and privacy protection under international human rights law.

The European Union's and United States' sides of the data localization debate have much to learn from each other, if only they would listen better. The European Union side should move beyond self-referential arguments based on E.U. law and pay greater attention to the question of whether data localization measures actually lead to greater protection in practice. And the United States side will have to take legal issues relating to the protection of individuals online more seriously and not just assume that all data localization measures have a protectionist agenda.

Data nationalism is not just a short-term political phenomenon subject to the ebbs and flows of protectionist sentiments, but the expression of a profound unease with the last few decades of increasing globalization, and of a lack of certainty on the part of society as to whether we want national borders carried over onto the online space. It can only be effectively countered by articulating a normative argument in favor of a free Internet. Chander and Lê have made a good start in this endeavor, but further work will be needed to turn back the tide of data nationalism.