Selected Papers of Internet Research 16:
The 16th Annual Meeting of the
Association of Internet Researchers
Phoenix, AZ, USA / 21-24 October 2015

ADVANCING POLITICAL AND ECONOMIC INTERESTS THROUGH DATA LOCALIZATION IN THE NAME OF PRIVACY AND SECURITY

Tatevik Sargsyan
American University

Abstract

Revelations about the US National Security Agency's mass surveillance programs presented an opportunity for foreign governments to push forward their Internet governance agenda. Many nation states proposed infrastructure-based initiatives to localize data within their jurisdiction citing concerns over privacy and security of their citizens. Relying on a conceptual framework that connects Internet infrastructure to power and social control this paper examines data localization proposals by a number of governments arguing that their purpose is to pursue alternative political and economic objectives in the name of privacy and security.

Extended Introduction

In the last two decades the world has witnessed ongoing battles between nation states, international institutions and private companies over control of the Internet. Scholars have addressed the question of who should control critical Internet resources and what economic and political advantage the control embeds. This paper, however, explores a different question. Instead of looking at who controls the Internet infrastructure, it looks at how nation states rely on Internet infrastructure to advance their political and economic goals in the name of privacy and security in the post-Snowden era.

The conceptual framework at the foundation of this paper is that technical architecture embodies power and can be an instrument to pursue various political and economic goals (DeNardis, 2012; Lessig, 1999). Well-known empirical evidence in support of this framework is instances of desperate regimes disconnecting their citizens from the global information infrastructure by choking off Internet connection. Such cases occurred during the civil unrests in the aftermath of the 2009 disputed Iranian presidential elections, as well as the uprisings in North Africa (Howard, Agarwal, & Hussain, 2011). Another example that captures the essence of this framework is surveillance, which is not only technologically imposed but also involves cooperation between governments and private companies (Balkin, 2014). More recently, increased privacy and security concerns following revelations about NSA surveillance have generated new government initiatives for data localization, once again encapsulating governments' desire to achieve goals relying on Internet infrastructure.

Suggested Citation (APA): Sargsyan, T. (2015, October 21-24) *Advancing Political And Economic Interests Through Data Localization In The Name Of Privacy And Security.* Paper presented at Internet Research 16: The 16th Annual Meeting of the Association of Internet Researchers. Phoenix, AZ, USA: AoIR. Retrieved from http://spir.aoir.org.

The term “data localization” broadly refers to any initiative limiting the collection, storage, and transfer of data based on jurisdiction. Most commonly, “data localization” takes the form of legal restrictions on data location and export, such as when an e-mail or cloud computing service is required to physically locate servers containing data belonging to a country’s residents within that country’s jurisdiction. Efforts to create national e-mail services, or cloud servers dedicated to support country- level networks are also drivers of data localization (Chander & Le, 2015; Hill, 2014). Governments may pursue a variety of goals with data localization proposals ranging from enhanced privacy and security to economic development to making it easier to track and oppress dissidents. Often, the stated incentives are a cover for alternative political and economic objectives. To set the stage for further exploration of such objectives, it is necessary to understand the relationship between large private companies that manage Internet infrastructure and governments.

Global Information and Communication Technology (ICT) companies operating the Internet’s material and virtual infrastructure have helped create universal and interoperable networks of communication, which have promoted access to knowledge and empowered individuals to advocate for their rights. These networks have also increased economic activity across jurisdictions by providing services to various industries, enabling digital trade, raising competition and reducing costs (Benkler, 2006; Castro & Mcquinn, 2015). At the same time, by facilitating information flow and managing huge amount of data, these companies and the data they host have inadvertently become targeted by governments.

Generally, governments cannot easily influence and control data flow without ICT companies’ mediation, which has been demonstrated by governments’ growing reliance on Internet infrastructure to enact law enforcement, surveillance, and control of communication. Many of the large ICT companies whose services are most used globally are headquartered in the United States, and not only subject to US anti-terrorism and surveillance law but also to US government pressure to promote its national security, and political and economic interests. It is no secret that the US government has been able to build backdoors to private companies’ communications data to engage in unwarranted mass surveillance, espionage, and cyberattacks on foreign governments and companies (Deibert, 2013; Greenwald, 2014).

In this context, foreign governments have long realized that they do not always have the leverage to influence decisions by US-based ICT companies, associating the latter with the US government interests (Mueller, 2010). Moreover, a variety of governments around the world have continuously expressed concerns about the reliance on ICT infrastructure that disproportionately flows through the United States. As an alternative, they have promoted the creation of local networks. These governments, however, gained new leverage over ICT companies and the US government when the Guardian revealed National Security Agency (NSA) consultant Edward Snowden’s leak of classified documents in 2013, including a secret cooperative agreement between US intermediaries and the US government (Ball, 2013; Greenwald, 2014).

The NSA surveillance scandal allowed foreign governments to question the legitimacy of US companies and the US government in promoting and protecting privacy and security of global Internet users, and to justify a renewed push for infrastructure-based initiatives to localize data within their borders as the most reasonable solution to resolve concerns over privacy and security. To explore this phenomenon, this paper takes a case study approach to review data localization initiatives by both democratic and non-democratic nation states, such as China, Russia, Germany, and France, and delivers a thorough analysis of the unstated incentives behind those initiatives, and subsequent implications.

Despite the outrage with which these countries responded to the NSA spying revelations, and promised to ensure enhanced privacy and security to their citizens, data localization is hardly the answer. These countries engage in their own extensive surveillance programs, often with little oversight, and would greatly benefit from access to more localized data about domestic citizens' social, economic, and political activities. Moreover, even in States where privacy laws are stricter, they can be overridden in the name of national security, public safety and crime.

Governments' arguments that data localization will keep foreign surveillance at bay are also subject to question. Foreign intelligence agencies often focus their surveillance activities abroad, relying on various malware and surveillance technologies that hack into systems. Under such circumstances, locating servers inside a country will not hinder foreign governments from engaging in espionage and gaining economic and political advantage. Moreover, data localization does not prevent states from collaborating and regularly sharing data with each other.

Data localization will also increase security risks for Internet users. The decentralized nature of cloud systems allows companies to provide better security; while on the other hand centralizing data in one location creates a "single point of failure," making the data more vulnerable to hacking attacks, criminal breaches and technical outages. Thus, user privacy and security will only depend on the available technologies and their lawful deployment, and the ability of authorities to get access to data rather than their location.

Hence, this paper argues that many nation states, including the case studies discussed in this paper, use privacy and security protection as a proxy to advance alternative interest. Instead, governments' incentives to increase security and privacy of their citizens can be achieved through strengthening the infrastructure of international Internet companies without compromising the inherent nature of the global and universal Internet through data localization.

The industry deploys two technical approaches to enhancing privacy protection: privacy enhancing technologies (PETs) and Privacy by Design (PbD). PETs are applications to manage various dimensions of privacy, such as anonymity and confidentiality. Privacy by Design is a more systematic approach to designing technology that carries desirable values (Borking & Raab, 2001; Cavoukian, 2012). Potentially, PETs and PoD can shift the focus of privacy protection from data localization to the prevention of unauthorized data access by governments.

Additionally, since privacy and security are not only a function of technological solutions but also governments' ability to access data through overarching laws, technical “backdoors” and malware, it is necessary to continue to push back against broad surveillance capabilities domestically, and increase transparency.

References

Balkin, Jack. (2014). Old-School/New-School Speech Regulation. *Harvard Law Review, 127*(8), 2296-2342.

Ball, James. (2013). NSA's Prism surveillance program: how it works and what it can do | US news | theguardian.com. *The Guardian*. http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

Benkler, Yochai. (2006). *The wealth of networks: How social production transforms markets and freedom*: Yale University Press.

Borking, John J., & Raab, C. (2001). Laws, PETs and other technologies for privacy protection. *Journal of Information, Law and Technology, 1*, 1-14.

Castro, Daniel, & Mcquinn, Alan. (2015). Cross-Border Data Flows Enable Growth in All Industries: The Information Technology & Innovation Foundation.

Cavoukian, Ann. (2012). Privacy by design. *Report of the Information & Privacy Commissioner Ontario, Canada*.

Chander, Anupam, & Le, Uyen P. (2015). Data Nationalism. *Emory Law Journal, 64*(3).

Deibert, Ronald. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto, Ontario: McClelland & Stewart.

Denardis, Laura. (2012). Hidden Levers Of Internet Control: An Infrastructure-Based Theory Of Internet Governance. *Information, Communication & Society, 15*(5), 720-738.

Greenwald, Glenn. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York, NY: Metropolitan Books.

Hill, Jonah Force. (2014). *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders.* Paper presented at the the Hague Institute for Global Justice, Conference on the Future of Cyber Governance.

Howard, Philip N., Agarwal, Sheetal D., & Hussain, Muzammil M. (2011). The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation*. http://www.brookings.edu/research/papers/2011/10/dictators-digital-network

Lessig, Lawrence. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books