2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Technological Sovereignty: Missing the Point?

Tim Maurer
Open Technology Institute
New America
Washington, DC, USA
maurer@newamerica.org

Robert Morgus
Open Technology Institute
New America
Washington, DC, USA
morgus@newamerica.org

Isabel Skierka
Global Public Policy Institute
Berlin, Germany
iskierka@gppi.org

Mirko Hohmann
Global Public Policy Institute
Berlin, Germany
mhohmann@gppi.net

Abstract: Following reports of foreign government surveillance starting in June 2013, senior officials and public figures in Europe have promoted proposals to achieve "technological sovereignty". This paper provides a comprehensive mapping and impact assessment of these proposals, ranging from technical ones, such as new undersea cables, encryption, and localized data storage, to non-technical ones, such as domestic industry support, international codes of conduct, and data protection laws. The analysis focused on the technical proposals reveals that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance.

Keywords: *international affairs, foreign policy, cyber security, technological sovereignty, surveillance, encryption*

1. INTRODUCTION

In the months following the 2013 reports revealing surveillance by foreign governments, European government officials and public figures have promoted a variety of measures for gaining "technological sovereignty." The current German government's coalition agreement, for example, explicitly states that it will "take efforts to regain technological sovereignty."[1]

Technological sovereignty has been used as an umbrella term to suggest a spectrum of different technical and non-technical proposals, ranging from the construction of new undersea cables to stronger data protection rules. Many of them are not new but have developed greater political traction over the past year.

The main contribution of this paper is a comprehensive, systematic mapping and impact assessment of these technological sovereignty proposals.[2] Non-technical proposals such as a restructured Safe Harbor Agreement or a new European Union Data Protection Directive are also part of the debate and pose pros and cons of their own. However, that is outside the scope of this paper, which focuses on the technical measures and whether they will actually protect against foreign surveillance and gauge their impact on the open and free Internet. It builds upon existing literature,[3] but differs by distinguishing between types of proposals, and by considering whether they achieve their purported goal of protecting against foreign surveillance. This paper goes beyond analyses focused solely on data localization requirements[4] by providing a comprehensive overview of the proposals that have been advanced under the umbrella of technological sovereignty.

Research on the implications of these technological sovereignty proposals remains nascent. A growing body of literature examines the growth of "data localization" policies, meaning the "laws and guidelines which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, and companies."[5] Such proposals were the focus of attention in early 2014, because they were part of Brazil's debate over its Internet Bill of Rights, "Marco Civil da Internet." The term "technological sovereignty" remains vague. As it is used by European policymakers, it resembles terms like "data sovereignty," which has been defined as "a spectrum of approaches adopted by different states to control data generated in or passing through national [I]nternet." It is a subset of "cyber sovereignty," which is "the subjugation of the cyber domain to local jurisdiction."[6]

Our analysis builds on the scholarship and approach of Internet governance expert Laura DeNardis, who writes, "arrangements of technical architecture are also arrangements of power."[7] The Internet is a meta-network, composed of a constantly changing collection of individual networks and devices that communicate with each other through the Internet Protocol (IP). Through technical features, the physical and software architecture, or code, shapes human behavior on the Internet and beyond. Because the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. This architecture constitutes a powerful tool for actors to further their interests. Code "sets the terms upon which [actors] enter, or exist, in cyberspace."[8] According to Stanford law professor Barbara van Schewick, policymakers who traditionally used the law can now use Internet technologies to bring about desired political or economic effects.[9] Building upon this scholarship, we designed a framework for classifying the proposals based on what part of the Internet they impact.

Our research identified proposals from over a dozen countries in Europe, ranging from technical ones, like localized or nationalize routing schemes, to non-technical ones, like a European wide data protection authority. The majority of proposals are from Germany. They come from academia, the government, and the private sector and differ even within government as different ministries brought forth different proposals. Upon further examination of the technical proposals, our analysis shows that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance and ideas like the expansion of encryption tools that are more effective at securing data.

2. METHODOLOGY

We began this research by collecting proposals and statements[i] by European political decision-makers, as well as those of stakeholders from the private sector and academia, made after June 5, 2013, the day on which the first wave of articles about government surveillance was published.[ii] It is important to bear in mind that while these proposals were advanced in response to the surveillance affair, they address different dimensions of a complex problem, namely the protection of (1) government secrets; (2) individual citizens' privacy; and (3) industry secrets. An additional complexity is the fact that policymakers have been using the political attention to suggest new industrial policies aimed at supporting the European Information Technology (IT) sector through major public investments and IT sector-specific subsidies.

Upon completing the desk based collection phase of research, we proceeded in three steps to determine how each proposal affects the governing structures of the Internet, different types of data, and the Internet's underlying architecture.

Step 1: Dividing proposals into Two General Categories – Technical and Non-Technical

A first review of the proposals revealed that they could be clustered into two general groups: technical and non-technical proposals. We then grouped technical proposals based on the type of technological change proposed: new undersea cables, national e-mail, localized routing, encryption, and localized data storage. These proposals directly affect the technical architecture of the Internet. Non-technical proposals are those that affect the Internet in other ways – for example, calls for new laws or for more transparency, which could affect the technical architecture but indirectly so.

Technical proposals are based on the type of technological change proposed: new undersea cables, national e-mail, localized routing and storage, and encryption. New undersea cables, for example, refer to suggestions to directly connect Latin America and Europe, avoiding data transfer through the United States. Likewise, national e-mail was suggested in Germany as a means of avoiding contact with American servers whenever possible. Localized routing goes a step further than national e-mail, in the sense that it would encompass all data, not just e-mail data, and route it solely through local servers. However, localized does not necessarily mean that the data is concentrated in one country. For example, localized could encompass the

[i] These proposals and their sources are detailed in Figure 2.

[ii] For greater detail on this topic, see: Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

entirety of the European Union. Finally, there have been calls for improving encryption, making existing encryption more accessible to the general public, and extending it to mobile devices.

Non-technical proposals are sorted based on the changed mechanism: institution, law, norm, transparency, and business. The idea to establish a single EU Data Protection Agency exemplifies how actors consider institutions as a means of addressing a given challenge. A wide variety of laws have been proposed, and some implemented, ranging from changes to the US-EU Safe Harbor agreement[10] to domestic data protection laws. There are also several proposals aimed at increasing trust – not through regulation, but through the establishment of common norms, like a "no-spying" agreement between the US and European partners.[11] Another non-technological category is composed of proposals aimed at increasing transparency of how governments and businesses handle the data of citizens and customers. Proposals to advance the national production of hardware and software mainly originate in Germany, such as the "IT Security Made in Germany" brand or the production of an IT-Airbus in cooperation with France. Ideas like these fall into the business cluster, though there are technical components to the proposals. Generally, these non-technical proposals impact non-technical factors that shape the Internet, like laws, norms, markets, and institutions.

For the purposes of this paper, we focus on the proposals that have the highest likelihood of impacting the technical functionality of the Internet, which we call technical proposals.

Step 2: Determining Proposals' Political Traction

Some proposals have gained more political traction than others over the past year and a half. For our purposes, high political traction means that proposals have been widely discussed and have been implemented, or plans for implementation have been set. Other proposals have been discussed, but their implementation remains uncertain. These are classified as having medium political traction. Some proposals have been barely discussed or were discussed and discarded, and these are classified as having low political traction.[iii]

Step 3: Integrating Different Types of Data: Data in Motion, Data at Rest, and Metadata

To elevate the level of technical acumen informing this debate, it is important to note that several types of data exist: data in motion, data at rest, and metadata. Governance proposals depend on what type of data is to be governed.

The data we access on the Internet is stored on servers. When this data is inactive – meaning, it is not being changed or in motion – it is classified as data at rest. Data at rest can be the text, music, or video files we store in the cloud, or the data that is the content of a webpage stored on a company server.

Data in motion is data that traverses the physical infrastructure of the Internet. Because the Internet is a global network of computing devices, from laptops and PCs to smart phones, data must flow from the host device or server to the device trying to access it. The easiest way to explain this phenomenon is to picture an e-mail sent from one user to another. The sender generates the data that then travels over the cables and wires that make up the physical

[iii] We explain the degree of political traction of the technical proposals in the Impact Analysis, section 3.

infrastructure of the Internet, until it reaches the intended recipient. The same process happens when a user tries, for example, to access content through a webpage or download videos from a server. The route taken by the data depends on a number of factors, ranging from physical constraints like bandwidth to contractual considerations like peering agreements. Nonetheless, data is generally routed through what technologists refer to as the "cheapest" route. This ensures that the data reaches its recipient quickly and keeps Internet speeds high for everyone.

Metadata, simply put, is the data about data. Two types exist. Structural metadata "indicates how compound objects are put together."[12] This type of metadata is mostly used to present complex items. Structural metadata takes two separate streams of data, identifies them, and then ensures that they are properly synchronized for presentation. In other words, structural metadata ensures that the visual stream of the latest movie you are watching is synchronized with the audio stream. The second type of metadata is descriptive metadata, which "describes a resource for purposes such as discovery and identification."[13] This is the conceptualization of metadata. Descriptive metadata allows users to query databases and to identify data based on relevant criteria. It should be noted that even encryption does not necessarily protect metadata from surveillance. Figure 2 visualizes how the proposals are clustered.

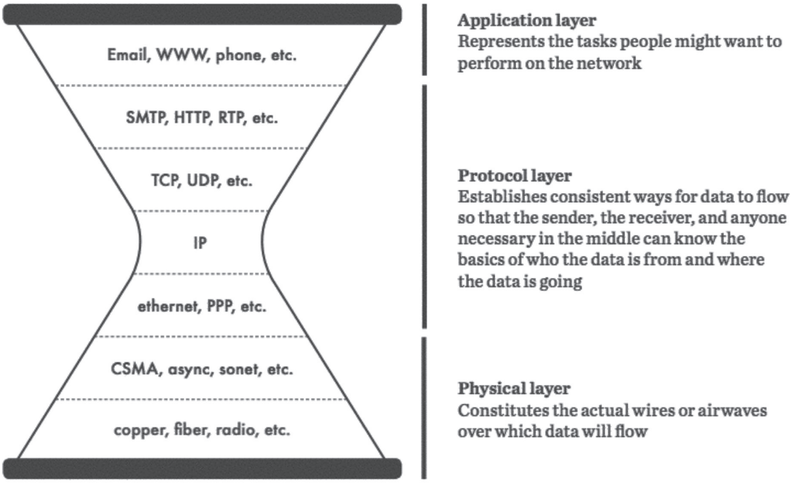
Step 4: Zooming in on Data in Motion: the Hourglass Model

Several models exist to illustrate the intricacies of the technical architecture that underlies the Internet. Internet expert and Harvard law professor Jonathan Zittrain built upon those and the work of many other scholars by combining the technical and social components of the Internet with his interpretation of the Hourglass Model, which highlights the centrality of the IP for the Internet's coherence and interoperability.

At the bottom is the physical layer, or "the actual wires or airwaves over which data will flow."[14] Undersea and fiber-optic cables are physical examples of the physical layer, as are the servers that receive them and the satellites that transmit a limited amount of Internet traffic. Next is the protocol layer, which "establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of whom the data is from and where the data is going."[15] This layer includes the limited IP, as well as the HTTP and the Simple Transportation Management Protocols (STMP). The IP layer is the narrowest layer in the hourglass model, signifying that it is, for the time being, the least elastic feature of the Internet, but also the layer on which the rest rely for communication. While we can build new cables and add more end-user devices, we are constrained by a finite number of IP addresses. Moving up the Hourglass, we find the application layer, "representing the tasks people might want to perform on the network."[16] E-mail clients and websites, for example, make up this layer. Resting atop the Hourglass are Zittrain's final two layers: the content layer, which is the actual information exchanged through the other layers, and the social layer, "where new behaviors and interactions among people are enabled by the technologies underneath."[17] These layers and the implications they carry apply directly to the proposals that we classify as technical proposals.

The architecture constraint in real space is the constraint of code in cyberspace. As the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. That’s why the technical proposals are a specific focus of this paper.

FIGURE 1: THE HOURGLASS MODEL


Email, WWW, phone, etc.
SMTP, HTTP, RTP, etc.
TCP, UDP, etc.
IP
ethernet, PPP, etc.
CSMA, async, sonet, etc.
copper, fiber, radio, etc.
Application layer
Represents the tasks people might want to perform on the network
Protocol layer
Establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of who the data is from and where the data is going
Physical layer
Constitutes the actual wires or airwaves over which data will flow

Source: Zittrain, Jonathan (2008) *The Future of the Internet and How to Stop It*. Yale University Press. p. 67-68.

FIGURE 2: TECHNICAL PROPOSALS

Type of Proposal	Summary	Proposing Actors	Country or Region	Time Range	Data Type	Layer	Political Traction
New Undersea cables	Lay a new fiber-optic submarine cable between Latin America and Europe; lay a new fiber-optic cable between Finland and Germany, circumventing Sweden[18, 19]	Public: Herman Van Rompuy[iv] Krista Kiuru[v]	EU, Finland	12/11/2013 - 2/24/2014	Motion	Physical	High
Localized routing	Data streams should flow within a geographically restricted zone; inter-Schengen data traffic should be routed within the Schengen zone[20, 21, 22, 23, 24, 25]	Public: German government Private: Deutsche Telekom, Atos	France, Germany	10/12/2013 - 7/27/2014	Motion + Meta	Protocol (Content, Application, Physical)	Medium

[iv] President of the European Council.

[v] Finnish Minister of Education, Science and Communication.

National e-mail	Route all e-mails within Germany on German servers and cables[26]	Private: Deutsche Telekom	Germany	8/1/2013	Motion + Meta	Applica-tion	High
Localized data storage	Create a European or a Schengen cloud; create a European or Schengen zone for data[27, 28, 29, 30]	Public: French, German governments Private: Green,[vi] Deltalis,[vii] Quantique,[viii] EuroCloud[ix]	France, Germany, Poland, Switzerland	6/27/2013 - 5/14/2014	Rest + Meta	Data at rest	High - Medium
Expansion of encryption tools	End-to-end encryption of communication data; encryption of end devices;[31, 32, 33] End-to-end mobile voice encryption;[34, 35] Secure SIM data for corporate customers[36]	Public: European Parliament, Academia: Stefan Katzenbeisser,[x] Mark Manulis[xi]	Germany, UK	11/23/2013 - 2/24/2014	Motion + Rest	Protocol, Content, Applica-tion, Physical, and Data at rest	Medium

3. IMPACT ANALYSIS

This impact analysis examines whether the proposals actually achieve their purported goals of making data more secure in response to the surveillance debate, and then assesses the proposals' broader implications for the Internet, using the 2011 OECD Principles for Internet Policy-Making.[37]

The OECD principles provide concise guidance for policymakers crafting Internet policy, and they were designed to "help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives."[38] Given that the OECD member countries, as well as multiple other stakeholders, agreed upon these principles, they offer a useful anchor for transatlantic cooperation. We identified eight out of the 14 principles that are relevant to technological sovereignty and grouped them into four categories that constitute the foundation for our analysis of the proposals:[xii]

Human Rights:

OECD #1: Promote and protect the global free flow of information.

OECD #9: Strengthen consistency and effectiveness in privacy protection at a global level.

[vi] Switzerland.

[vii] Switzerland.

[viii] Switzerland.

[ix] Poland.

[x] Technische Universität Darmstadt, Germany.

[xi] University of Surrey, United Kingdom.

[xii] For a full list and explanation of the principles, see Annex 3 of Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

Governance – Open Internet:

OECD #2: Promote the open, distributed, and interconnected nature of the Internet.
OECD #8: Ensure transparency, fair process, and accountability.

Economic:

OECD #4: Promote and enable the cross-border delivery of services.
OECD #11: Promote creativity and innovation.

Security:

OECD #13: Encourage cooperation to promote Internet security.
OECD #14: Give appropriate priority to enforcement efforts.

New Undersea Cables

Public sector officials have suggested laying new undersea cables in order to circumvent foreign surveillance. Laying new undersea cables alters the physical layer of the Internet's architecture over which data will flow and does not harm the free flow of information *per se*. However, new undersea cables are not an effective strategy to protect against foreign surveillance because foreign law enforcement and intelligence agencies are adept at tapping undersea cables.[39] Thus, proposals for new undersea cables as a means to avoid foreign surveillance creates a false sense of security for users. While new and more undersea cables can positively contribute to an interconnected and distributed Internet, they do not make data more secure.

Localized Routing

Parts of both the public and private sectors have suggested the implementation of localized routing. These schemes require the alteration of transmission protocols that dictate how data flows over the physical architecture of the Internet. However, despite physically altering the location of data flows, localized routing does not effectively protect data from foreign surveillance. For this reason, legally mandated localized routing schemes have lost nearly all their political traction in Europe. It would also make law enforcement easier, as data would be subject to national data protection laws, which usually contain law enforcement exemptions.[40] Therefore, the localization of routing is unlikely to actually secure communications and risks providing a false sense of security to Internet users.

Mandatory localized routing requirements could also have dire consequences for the Internet as a whole. It would require changes to the routing protocols and IP address allocation system, contra to one of the Internet's fundamental principles that data flows via the cheapest or most efficient route. Whether or not a localized routing scheme negatively affects the free flow of information depends on the rule of law in the location in question. This enhances domestic private and state actors' control over information and data flows, and several authoritarian regimes have sought to implement localized routing to increase their own control over data flowing across the Internet infrastructure geographically located within their country.[41] It should be noted that there has also been a debate about "Network Security Agreements" between the U.S. government and foreign telecommunications providers, such as Deutsche Telekom, to localize routing of national data traffic.[42]

National E-Mail

National e-mail schemes, like E-Mail Made in Germany, were proposed and implemented by both Deutsche Telekom and United Internet, who are serving more than two thirds of e-mail users in Germany.[43] However, because the proposed service does not use a higher than normal security standard to this date it will not protect against surveillance any better than existing services of which many have used the Simple Mail Transfer Protocol Secure (SMTPS) with Transport Layer Security (TLS) for years already.[44] Moreover, the E-Mail Made in Germany initiative has been criticized for using a proprietary standard for secure data transmission (the "Inter Mail Provider Trust") instead of the openly available standard DANE (DNS-Based Authentication of Named Entities), which other smaller competitors have been using and is more easily auditable.[45] Finally, if data is stored unencrypted on the e-mail provider's servers, it can still be intercepted regardless of the encryption used for the data in transit.

National e-mail could in fact make law enforcement easier, since data is stored within national borders and subject to national data protection laws, which usually contain enforcement exceptions.[46] The proposed service highlights the risk of promoting proposals that give users a false sense of security by claiming enhanced security features without actually significantly enhancing security.

Localization of Stored Data

Both public and private sector officials have proposed mandating localized data storage. Proposals to territorially localize data storage seek to store all data generated by Europeans on servers located in Europe. This action will not effectively protect data from surveillance and actually concentrates the data in a number of defined physical locations, potentially narrowing the search for intelligence and law enforcement agencies seeking specific data.

Adding to that, legal barriers for foreign intelligence agencies are often less strict when collecting data internationally. Although data stored in Europe is subject to EU data protection laws, this does not mean that the parties that own the data are exclusively subject to those same laws. Therefore, the security of data from foreign intelligence agencies depends not on where it is stored, but on comprehensive security practices, modern technology, and qualified security personnel.[47] Similar to other localization proposals, it risks providing a false sense of security to users.

Localized data storage would also harm the open and distributed nature of Internet, by forcing the "nodes" to be located in specific geographic areas, where their operations might be suboptimal from a global perspective.

Requiring localized data storage would impede cross-border delivery of services and raise costs and barriers to entry, particularly for smaller companies, which in turn risks hampering innovation.[48]

For these reasons, no steps have been taken to date to legally mandate localized data storage. Instead, policymakers have turned to the promotion of voluntary data security standards. For example, the European Commission issued the Common Service Level Agreements for Cloud Computing[49] and the European Cloud Partnership, which suggest common, non-binding security and encryption standards for European cloud providers storing data on European soil.[50]

Expansion of Encryption Tools

Suggestions to expand encryption tools have come from the public sector and academia. While encryption may not protect individuals against sophisticated, targeted surveillance by intelligence agencies, the widespread use of encryption would significantly raise the cost of surveillance generally. The more individuals encrypt their communications, the more difficult and costly it will to decrypt those communications. Encryption can be applied to all layers of the Internet – to the physical layer (cable or radio communications), the protocol layer (i.e, Hypertext Transfer Protocol [HTTP] or Transmission Control Protocol [TCP]), and the application layer (e-mail, www, mobile). Thus, encryption can protect both data in motion through end-to-end encryption of communications, as well as data at rest through encryption of devices or servers at the end nodes.

Calls for stronger encryption have received growing political traction around the world. Several experts have called for the development of more easily accessible encryption tools,[51] and the European Parliament has called on the European Commission to "strengthen the protection of confidentiality of communication … by way of requiring state-of-the-art end-to-end encryption of communications."[52] Major technology companies like Apple and Google have also begun offering encryption by default,[53] and the Internet Engineering Task Force (IETF) has resumed work on building encryption by default into HTTP 2.0 after the initial surveillance reports, a project it had previously decided against in March 2012.[54]

The different forms of encryption tools proposed in Europe attempt to deliver better privacy through end-to-end encryption of mobile voice communication. The use of crypto phones can be an effective tool for protecting government and business secrets and individuals' private data. Various proposals also advocate for better end-to-end encryption of e-mail, instant messaging, cloud storage, and radio. Existing tools are often difficult and cumbersome to use, so engineers at the IETF and major US software companies are working on making encryption more easily accessible to the wider public.[55] It is possible for data encrypted from end-to-end to be accessed by intelligence or law enforcement agencies, but only through measures targeted at specific users and with much greater difficulty. While encryption enhances the protection of both data in motion and at rest, it does not necessarily protect metadata.

Different forms of encryption can be applied to various layers of the Internet while preserving its decentralized structure and strengthening the capacity of actors within the existing frameworks. Therefore, the use of encryption tools has no negative impact on the free flow of information. As long as encryption is promoted globally and encryption tools can be imported and exported without national restrictions, proposals to enhance encryption efforts can promote innovative, easier-to-use technologies. The use of encryption technologies strengthens overall Internet security, as well as individual and collective efforts for self-protection. However, encryption proposals are not without drawbacks.

First, encryption tools are generally regarded as difficult and cumbersome to use and adoption of strong encryption, though available, has been slow.[56] Second, law enforcement and counterterrorism agencies point to a tension between data privacy and national security and law enforcement.[57] Law enforcement in the United States, in particular, has argued that the expansion of encryption lends itself to the "going dark" problem and severely hinders law enforcement investigations.[58] Some have consequently advocated for a "golden key" to encrypted devices and communications, which should be provided to or stored with a third party, such as a trusted authority under the state's jurisdiction. However, such backdoors and keys stored elsewhere constitute a risk for Internet security, since they could be exploited by criminals.[59] This topic and how to approach physical and virtual security has been the subject of an emerging and important debate in the United States and the United Kingdom.[60]

4. CONCLUSION

Calls for technological sovereignty have not been limited to Europe. In Brazil, data localization proposals were hotly debated. In China, government offices are prohibited from using the Windows 8 operating system, and Cisco and IBM are under scrutiny.[61] The Australian government has banned China's Huawei from participating in building its National Broadband Network. And the United States has not been immune from this trend, as portrayed by Congress's creation of a cyber espionage review process in 2013 to limit government procurement of Chinese IT equipment.[62] Moreover, under "Network Security Agreements," the U.S. government legally obliges foreign communication infrastructure providers such as Deutsche Telekom to route their traffic exclusively within U.S. borders.[63]

This in-depth analysis of the European technological sovereignty proposals reveals several trends. First, it is unlikely that most technical proposals proposed to date will effectively protect data against surveillance from foreign government intelligence agencies. Only a limited number of proposals might achieve that – namely encryption – and they have not been at the center of attention in the European debate. Second, some proposals could in fact have a negative effect on the open and free Internet, or at least lead to an inefficient allocation of limited resources. Moreover, the specific impact often depends on how the proposals are implemented and remains uncertain without further research. Third, the proposals tend to be narrowly focused on the transatlantic dimension and generally neglect the larger challenge and the new technological reality. Finally, especially in the case of the expansion of encryption tools, tensions between privacy advocates, private companies, and law enforcement and national security officials emerge.

The impact of proposals often depends on the details of their implementation, which remain unknown to date. On the surface, a proposal might appear to have a positive impact but a closer look casts doubt on their effectiveness. For example, increasing funding for small businesses and establishing an "IT Security Made in Germany" brand will only increase data security if those companies produce, and are capable of producing, products and services with higher security standards than those of foreign companies. So far, the implementation of these proposals does not suggest that they offer significantly more secure services, which in some cases instead provides a false sense of security.

At first blush, restricting data from flowing through the physical infrastructure of other countries might seem like an effective measure for protecting against government surveillance. However, this is a false hope. Moreover, the laws in some countries lower the legal barrier for intelligence agencies to collect and analyze data if the data is collected outside of the intelligence agency's home country.[64] This reality means that measures forcing data to remain within a country's borders might lower the legal threshold for foreign intelligence agencies to conduct surveillance in the first place. Proposals focused on simply physically avoiding certain countries misunderstand current technological and legal realities and risk wasting important resources that could be used to effectively make data more secure.

Data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted. A critical fact often ignored in the debate thus far is that the governments exposed by media reports since June 5, 2013 are unlikely to be the only countries with such technical surveillance capabilities. The issue is global, not Transatlantic, in nature and the challenge is the result of a new technological reality. It therefore requires a broader debate and approach. The proposals most likely to protect against any foreign surveillance focus on encryption tools. These deserve greater attention and scrutiny if the goal is to secure data more effectively.

ACKNOWLEDGMENT

The authors would like to thank the members of the Steering Committee for the project Transatlantic Dialogues on Security and Freedom in the Digital Age (go to www.digitaldebates.org for more) as well as the participants of the workshops hosted in Washington, DC, and Berlin for their valuable input and feedback. All views, errors or omissions are solely the authors' responsibility.

REFERENCES

[1] German Government. 2013. "Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode." <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=2820F3157BAD69B7313E63020CF9944C.s4t2?__blob=publicationFile&v=2>.

[2] A comprehensive list of proposals can be found in Annex II.

[3] Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders." *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>; Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet." *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[4] Chander, Anupam and Uyen P. Le. 2014; Hill, Jonah Force. 2014.

[5] Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders." *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>.

[6] Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet." *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[7] DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press, p. 9.

[8] Lessig, Lawrence. 1998. "The Laws of Cyberspace." *Presented at the Taiwan Net '98 Conference*. p. 4.

[9] van Schewick, Barbara. 2010. *Internet Architecture and Innovation*. Cambridge: MIT Press.

[10] The Safe Harbor agreement is the process developed by the US Department of Commerce that allows US companies to more easily comply with EU Directive 95/46/EC, the initial EU Data Protection Directive from 1998. When the directive went into force in 1998, "it became clear that it actively threatened data flows between the two largest trading partners on earth." Thus, the Safe Harbor agreement, which is unique to the US and EU, is "voluntary self-certification system for transmitting data from the EU to the United States." For more on the Safe Harbor, see: Dowling, Jr., Donald C. 2009. "International Data Protection and Privacy Law." *White & Case*. p. 12. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[11] O'Donnell, John and Baker, Luke. 2013. "Germany, France demand 'no-spy' agreement with U.S." *Reuters*. Oct. 24. <http://www.reuters.com/article/2013/10/25/us-eu-summit-idUSBRE99N0BJ20131025>.

[12] National Information Standards Organization. 2004. *Understanding Metadata*. NISO Press, p. 1-2. <http://marciazeng.slis.kent.edu/metadatabasics/types.htm>.

[13] Ibid.

[14] Zittrain, Jonathan L. 2008. *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press, Chapter 4, p. 67-100.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] European Council: The President. 2014. "Press Statement by the President of the European Council, Herman Van Rompuy, following the 7th EU-Brazil Summit." *The European Council*. <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf>.

[19] Ronnholm, Antton. 2014. "Minister Kiuru on submarine cable decision: Finland to be a safe harbor for data." *Finnish Ministry of Transport and Communications*. Apr. 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>.

[20] Berke, Jürgen. 2013. "Telekom will innerdeutschen Internetverkehr ubers Ausland stoppen." *Wirtschafts Woche*. Oct. 12. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html>.

[21] Schäfer, Louisa. 2013. "Deutsche Telekom: 'Internet data made in Germany should stay in Germany.' Interview with Philipp Blank." *Deutsche Welle*. Oct. 18. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>.

[22] Gaugele, Von Jochen, Kade, Claudia, Malzahn, Claus Christian and Vitzthum, Thomas. 2014. "Dobrindt will mit 'Netzallianz' an die Weltspitze." *Die Welt*. Jan. 12. <http://www.welt.de/politik/deutschland/article123774038/Dobrindt-will-mit-Netzallianz-an-die-Weltspitze.html>.

[23] Thombansen, Hannah. 2014. "Video-Podcast der Bundeskanzlerin #2/2014." *Bundesregierung*. Feb. 15. <http://www.bundesregierung.de/Content/DE/Podcast/2014/2014-02-15-Video-Podcast/links/download-PDF.pdf;jsessionid=0BC9A500E8D948E37C285341160692B2.s4t1?__blob=publicationFile&v=3>.

[24] Breton, Thierry. 2013. "Atos CEO calls for 'Schengen for data." *Thierry Breton's blog*. Sept. 2. <http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>.

[25] von Altenbockum, Jasper und Lohse, Eckart. 2014. "Verfassungsschutz-Präsident 'Wir werden unsere Abwehr verstärken.'" *Frankfurter Allgemeine Zeitung*. July 28. <http://www.faz.net/aktuell/politik/inland/interview-mit-hans-georg-maassen-abwehr-verstaerken-13067331.html>.

[26] Deutsche Telekom. 2013. "Deutsche Telekom, WEB.DE and GMX launch 'E-mail made in Germany' initiative." *Deutsche Telekom Media*. Aug. 9. <http://www.telekom.com/media/company/192834>.

[27] Iwankiewicz, Maciej W. 2013. "The Polish Approach to EU Cloud Computing Strategy." *EuroCloud*. July 5. <http://www.eurocloud.org/the-polish-approach-to-the-eu-cloud-computing-strategy/>.

[28] Deutscher Bundestag. 2013. "Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit." *German Bundestag*. Nov. 15. <http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf>.

[29] Juskailian, Russ. 2014. "For Swiss Data Industry, NSA Leaks Are Good as Gold: here's how the Swiss promise to keep your data safe." *Technology Review*. Mar. 18. <http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/>.

[30] Le Maire, Bruno. 2014. "Bruno Le Maire: Pour un Cloud europeen." *Slate*. May 14. <http://www.slate.fr/tribune/87057/bruno-le-maire-cloud-europeen>.

[31] European Parliament. 2014. "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." Feb. 21. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[32] Ward, Mark. 2014. "Can Europe go its own way on data privacy?" *BBC Technology*. Feb. 17. <http://www.bbc.com/news/technology-26228176>.

[33] Schutz, Colin. 2014. "Tech Companies Are Trying to Make NSA-Proof Encrypted Phones and Apps." *Smithsonian Magazine*. Feb. 24. <http://www.smithsonianmag.com/smart-news/tech-companies-are-responding-nsa-revelations-encrypted-phones-and-apps-180949874/?no-ist>.

[34] Sawall, Achim. 2013. "Simko 3 zugelassen." *Golem.de*. Sep. 9. <http://www.golem.de/news/simko-3-zugelassen-hintertueren-lassen-sich-bei-smartphones-nicht-ausschliessen-1309-101467.html>.

[35] Deutsche Telekom. 2013. "Data Privacy and Data Security: Report 2013." *Deutsche Telekom AG*. <http://www.telekom.com/dataprotection>.

[36] Gandhe, Shreyas. 2014. "Vodafone Germany starts rolling out SIM card based encryption." *Neowin.net*. Mar. 12. <http://www.neowin.net/news/vodafone-germany-starts-rolling-out-sim-card-based-encryption>.

[37] OECD. 2011. "Communiqué on Principles for Internet Policy-Making." *OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth*. June 29. p. 3. <http://www.oecd.org/internet/innovation/48289796.pdf>.

[38] Ibid.

[39] Khazan, O. 2013. "The Creepy, Long-Standing Practice of Undersea Cable Tapping." *The Atlantic*. Jul. 16. <http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>.

[40] Dowling, Jr., Donald C. 2009. "International Data Protection and Privacy Law." *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[41] See, for example: Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. "Internet Censorship in Iran: A First Look." *Censorship Project*. Aug. <https://jhalderm.com/pub/papers/iran-foci13.pdf>; and Roberts, Hal, David Larochelle, Rob Faris, and John Palfrey. 2011. "Mapping Local Internet Control." *Berkman Center for Internet & Society at Harvard University*. May 13. <http://cyber.law.harvard.edu/netmaps/mlic_20110513.pdf>.

[42] Public Intelligence. 2013. "U.S. Government Foreign Telecommunications Providers Network Security Agreements". <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[43] Deutsche Telekom. 2014. <http://www.telekom.com/medien/produkte-fuer-privatkunden/220370>.

[44] Dierks, T. and E. Rescorla. 2008. "The Transport Layer Security (TLS) Protocol Version 1.2." *Internet Engineering Task Force Network Working Group*. <http://tools.ietf.org/html/rfc5246>.

[45] Emert, M. 2014. "RIPE diskutiert bedenkliche Entwicklungen: Das Google-Net und EmiG". 19 May. < http://www.heise.de/netze/meldung/RIPE-diskutiert-bedenkliche-Entwicklungen-Das-Google-Net-und-EmiG-2192176.html>.

[46] Dowling, Jr., Donald C. 2009. "International Data Protection and Privacy Law." *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[47] Bob Butler, Irving Lachow, Jonah Force Hill. 2014. "Cloud computing under siege." *Few.com*. Sept. 12. <http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx>.

[48] Plaum, Alexander. 2014. "The impact of forced data localisation on fundamental rights." *Access Now*. April 4.. <https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights>.

49] European Commission. 2014. "Cloud Service Level Agreement Standardisation Guidelines". <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.

[50] European Cloud Partnership Steering Board. 2014. "Establishing a Trusted European Cloud." <http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf>.

[51] Waidner, Michael. 2014. "Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014." June 26. <https://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf>.

[52] European Parliament. 2014. "Motion for a European Parliament Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." *European Parliament*. Feb. 21. Paragraph 95. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[53] Vance Jr., Cyrus R. 2014. "Apple and Google threaten public safety with default smartphone encryption." *The Washington Post*. Sept. 26. <http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html>.

[54] Jackson Higgins, Kelly. 2013. "NSA Leaks Bolster IETF Work On Internet Security." *DarkReading*. Nov. 14. <http://www.darkreading.com/risk/nsa-leaks-bolster-ietf-work-on-internet-security/d/d-id/1140891>.

[55] Protalinski, Emil. 2014. "Gmail now always uses an HTTPS connection and encrypts all messages moving internally on Google's servers." *The Next Web*. Mar. 20. <http://thenextweb.com/google/2014/03/20/gmail-now-uses-encrypted-https-connection-check-send-email/>; Armasu, Lucian. 2014. "Huge: Cloudflare's Free SSL Service Brings Encrypted-By-Default Web Closer Than Ever." *Tom`s Hardware*. Sept. 29. <http://www.tomshardware.com/news/cloudflare-security-encryption-ssl-https,27780.html>; Perey, Juan Carlos. 2014. "Microsoft makes email encryption for Office 365 easier." *Tech Central.ie*. Oct. 6. <http://www.techcentral.ie/microsoft-makes-email-encryption-office-365-easier/#ixzz3Ix0eOXHl>; O'Neill, Patrick Howell. 2014. "Tor executive director hints at Firefox integration." *The Daily Dot*. Sept. 29. <http://www.dailydot.com/politics/tor-mozilla-firefox/>; Meyer, David. 2014. "Pretty Easy Privacy project aims to make encryption easier for regular people to use." *Gigaom*. Oct. 6. <https://gigaom.com/2014/10/06/pretty-easy-privacy-project-aims-to-make-encryption-easier-for-regular-people-to-use/>.

[56] For a broader discussion of the usability of encryption, see: Lee, Timothy B. 2013. "NSA-proof encryption exists. Why doesn't anyone use it?" Washington Post. June 14. <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/>.

[57] For more on this debate in the UK, see: Price, Rob. 2015. "David Cameron Wants to Ban Encryption." *Business Insider*. Jan. 12. <http://www.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1>.

[58] FBI Director James Comey has been particularly outspoken on this issue. For more, see: Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>.

[59] Schneier, Bruce. 2014. "Stop the hysteria over Apple encryption." *CNN*. Oct. 31. <http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/>.

[60] The Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *The Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>; Street, Jon. 2014. "Eric Holder: Apple, Google Not Giving Law Enforcement Access to Encrypted Data Is 'Worrisome.'" *The Blaze*. Oct. 1. <http://www.theblaze.com/stories/2014/10/01/ eric-holder-apple-google-not-giving-law-enforcement-access-to-encrypted-data-is-worrisome/>; Hosko, Ronald T. 2014. "Apple and Google's new encryption rules will make law enforcement's job much harder." *The Washington Post*. Sept. 23. <http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>.

[61] Tiezzi, Shannon. 2014. "In Cyber Dispute With US, China Targets IBM, Cisco." *The Diplomat*. May 28. <http://thediplomat.com/2014/05/in-cyber-dispute-with-us-china-targets-ibm-cisco/>.

[62] Rogers, Mike and Dutch Ruppersberger. 2012. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Permanent Select Committee on Intelligence. Oct. 8. <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>.

[63] Public Intelligence. 2013. "U.S. Government Foreign Telecommunications Providers Network Security Agreements". <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[64] Willis, Aidan. 2010. "Guidebook: Understanding Intelligence Oversight." *Geneva Centre for the Democratic Control of Armed Forces (DCAF)*. <http://www.dcaf.ch/Publications/Guidebook-Understanding-Intelligence-Oversight>.