"The Effects of Data Localization on Cybersecurity"

Peter Swire & DeBrae Kennedy-Mayo*

Table of Contents

I. Introduction

* Peter Swire is the Elizabeth and Tommy Holder Chair and Professor of Law and Ethics at the Georgia Institute of Technology, with appointments in the School of Cybersecurity and Privacy and the Scheller College of Business. He is Research Director of the Cross-Border Data Forum and senior counsel with the law firm of Alston & Bird. DeBrae Kennedy-Mayo is a research faculty member in the Scheller College of Business at the Georgia Institute of Technology. She is also a senior fellow with the Cross-Border Data Forum. The statements in this document are solely by the authors, and should not be attributed to the Cross-Border Data Forum or any client.

For research support on this project, the authors thank the Center for International Business and Education at Georgia Tech, the Cross-Border Data Forum, the Hewlett Foundation Cyber Project, Microsoft, and the Scheller College of Business. The authors thank Nathan LeMay for research on this project.

Cyber-attacks are global – they often originate continents away from the ultimate target. By contrast, laws are made nationally (or sometimes regionally, as in the European Union ("EU")). Many national laws elsewhere can affect the ability of those in one country to learn about or otherwise defend themselves against cyber-attacks.[1] This paper examines a prominent category of such laws – data localization laws.

The importance of data localization has risen rapidly in recent years, including for the three major areas of China, the EU, and India. First, China's data security act took effect in 2017, requiring data localization for the broadly defined sector of critical infrastructure.[2] Second, the European Union has taken significant steps toward data localization in the wake of the 2020 *Schrems II* decision of the European Court of Justice. Among recent enforcement actions, the Portuguese data protection authority ordered a government agency to terminate its use of cybersecurity services from U.S.-based Cloudflare.[3] Third, India has required data localization for financial transactions and is seriously considering doing the same for communications and other data.[4] As Nigel Cory and Luke Dascoli have recently documented, the number of data localization measures has roughly doubled in the past four years, including at least 62 countries with 144 restrictions.[5]

This paper focuses on the effects of *"hard" data localization*, where transfer of data is prohibited to other countries. Other "softer" versions of data localization also exist, such as where a country requires a copy of data to be stored or mirrored in the country, but transfer of the data remains lawful. Our discussion of localization includes both de jure and de facto effects – for instance China has passed explicit laws prohibiting data transfers, while the EU, pursuant to important guidance from the European Data Protection Board ("EDPB"), has taken important steps in practice toward de facto localization for the broad category of "personal data," which is approximately what is called "personally identifiable information" in the U.S.[6]

---

[1] "Technology is inherently global. … Policy is always jurisdictional." Bruce Schneier, *Technologists vs. Policy Makers*, 18 IEEE SEC. & PRIV. 72 (2020), at https://ieeexplore.ieee.org/document/8965265.

[2] Jinhe Liu, "China's Data Localization" (2020), at https://doi.org/10.1080/17544750.2019.1649289.

[3] Peter Swire & DeBrae Kennedy-Mayo, "New Urgency About Data Localization with Portuguese Decision," IAPP Privacy Perspectives, Apr. 29, 2021, at https://iapp.org/news/a/new-urgency-about-data-localization-with-portuguese-decision/#.

[4] Peter Swire et al., "India's Access to Criminal Evidence in the U.S." (2020), at https://www.orfonline.org/research/indias-access-to-criminal-evidence-in-the-us/.

[5] Nigel Cory & Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Fund, July 19, 2021, at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

[6] Nigel Cory, "How *Schrems II* Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime," Information Technology & Innovation Fund, July 8, 2021, at https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data.

The focus is also on *defensive cybersecurity* – effects on the ability of organizations such as corporations and government agencies to identify, protect, detect, respond, and recover in the face of cyber-attacks.[7] The paper does not seek to analyze other aspects of security, including offensive cyber measures and government surveillance used to protect national security.

To explore the effects of hard data localization, much of the discussion will use the example of the EU and will discuss potential data localization in India. One reason for the focus on the EU is that we have examined a useful data set about cybersecurity and the EU. In November, 2020 the EDPB issued draft guidance with a large localization effect,[8] and that guidance was finalized in mostly similar form in 2021.[9] Professor Théodore Christakis explained that this "EDPB Guidance seems nonetheless to prohibit almost all such transfers when the personal data is readable [i.e. non-encrypted] in the third country."[10] In earlier work, expanded upon here, we reviewed the approximately 200 public comments to the EDPB, about 25% of which raised the issue of data localization.[11] A second reason is that the EU and India illustrate one important finding: if there is exactly one country with a localization law, then data can be centralized in that country, facilitating centralized management of an organization's cybersecurity program. By contrast, if both the EU and India require localization, the organization can no longer centralize system management: data from the EU cannot go to India, and data from India cannot go to the EU.[12] *Although good cybersecurity practice integrates management of the organization's system, required localization in two or more nations restricts the ability to conduct integrated cybersecurity management – including information sharing of emerging cyberattacks, trend analysis, and remediation best practices.*

---

[7] The scope of defensive cybersecurity approximately matches the scope of the NIST Cybersecurity Framework, which addresses the five phases of "identify, protect, detect, respond, and recover." Cybersecurity Framework, NIST, at https://www.nist.gov/industry-impacts/cybersecurity-framework.

[8] European Data Protection Board, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Dec. 21, 2020), at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en.

[9] Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, European Data Protection Board (EDPB) (Jun. 18, 2021), at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[10] Theodore Christakis, "*Schrems III*? First Thoughts on the EDPB post-*Schrems II* Recommendations on International Data Transfers (Part 3)," European Law Blog (2020), at https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/.

[11] DeBrae Kennedy-Mayo & Peter Swire, "Prominent Theme of Data Localization in Comments to EDPB Guidance on Implementing *Schrems* Has New Urgency with the Portuguese Decision," Cross-Border Data Forum, Apr. 29, 2021, at https://www.crossborderdataforum.org/prominent-theme-of-data-localization-in-comments-to-edpb-guidance-on-implementing-schrems-ii-has-new-urgency-with-the-portuguese-decision/.

[12] Our thanks for this point to our student Nathan LeMay, who worked with us in early stages of this project.

Part II examines privacy and non-privacy reasons driving localization laws. The discussion begins by examining ways that cybersecurity might either reinforce privacy or exist in tension with it. We propose the following definition of possible conflicts between pursuing privacy and cybersecurity -- a measure designed to increase privacy reduces cybersecurity to the extent the privacy measure increases the risk of unauthorized access, reduces integrity, or reduces availability. The discussion next addresses non-privacy rationales for data localization, concluding that in general the rationale for localization does not alter the analysis of cybersecurity risks arising from localization.

Part III addresses the research methodology for this paper. In addition to a traditional literature review, which found no previous systematic discussion of these issues, we reviewed approximately 200 comments submitted to the EDPB in late 2020 concerning data transfers. Approximately 25% of the comments discussed data localization or a similar concept. Third, we analyze International Standards Organization ("ISO") 27002, as a way to systematically examine the effect of data localization on a widely-used set of cybersecurity controls.

Part IV provides a new categorization of the effects of data localization on cybersecurity. First, our analysis shows that data localization would threaten an organization's ability to achieve *integrated management of cybersecurity risk*. As shown in Appendix A, 13 of the 14 ISO 27002 controls, as well as multiple sub-controls, would be affected by data localization. Second, the analysis explains how data localization pervasively limits *provision of cybersecurity-related services by third parties*, a global market of roughly $200 billion currently, with doubling expected within a few years. Third, data localization threatens non-fee cooperation on cybersecurity defense. Notably, localization undermines *information sharing for cybersecurity purposes*, which policy leaders have emphasized as vital to effective cybersecurity. In our discussion of each of three effects of data localization on cybersecurity, we will briefly examine the primary counter arguments to our position. For instance, we will examine the arguments made that support the positions of countries that have adopted data localization or that are strongly considering implementing such requirements. Part V is the conclusion.

II. Data Localization for Privacy, Cybersecurity, and Other Reasons

For the EU, privacy and data protection laws are driving the current trend toward de facto data localization. The analysis here about the EU, in large measure, becomes a question about how this privacy regime can create risks for cybersecurity. As researchers in both privacy and cybersecurity, we are acutely aware that stronger privacy protections often improve cybersecurity, and stronger cybersecurity measures often improve privacy. With that said, our research shows significant and often underappreciated ways that the two goals can exist in tension with each other. We examine the interaction of privacy and cybersecurity in some detail, so that those who support both goals can more clearly see how localization rules adopted to protect privacy can indeed create cybersecurity risks.

We then briefly address other reasons driving localization laws, including but not limited to protectionist efforts to boost local industry. In general, the risks to cybersecurity result similarly from data localization limits, whatever the reason for adopting such limits. In addition,

as Cory and Dascoli have pointed out, the effects of localization can result either from explicit legal rules or de facto, "[b]y making data transfers so complicated, costly, and uncertain, firms basically have no other option but to store the data locally, especially in the face of massive fines."[13]

A. Data Localization for Privacy Reasons

As one of the authors (Swire) wrote back in 2002: "Both privacy and security share a complementary goal—stopping unauthorized access, use, and disclosure of personal information."[14] Effective security is required by Article 32 of GDPR, and is one of the fair information privacy principles: "After all, good privacy policies are worth very little if hackers or other outsiders break into the system and steal the data."[15] Preventing unauthorized access is a major part of "security *and* privacy."

Briefly, consider two major areas where privacy and security reinforce each other. First, encryption is a widely-used measure to enhance privacy, providing a technical basis for fewer people to access personal data. Encryption also enhances security, making it more difficult for unauthorized persons to access the data. European data protection experts have often emphasized the importance of strong encryption, as seen for example in a 2016 speech on cybersecurity by then European Data Protection Supervisor Giovanni Buttarelli.[16] Second, beyond encryption, there has been substantial work done on "privacy enhancing technologies," ("PETs") including by the European Union Agency for Cybersecurity ("ENISA").[17] In its discussion of PETs, ENISA highlights "data minimisation, anonymisation, and pseudonymisation."[18] These PETs help privacy because fewer recipients see the personal data, except where there is a need for the recipient to have access to that data. These PETs help cybersecurity because they reduce the likelihood of breach (fewer places store personal data) as well as the likely cost of a breach (a breached dataset contains less sensitive data).

With full cognizance of the ways that privacy and security reinforce each other, they can also come into conflict.[19] Although providing one definition of "privacy" is notoriously

---

[13] Cory & Dascoli, *supra.*

[14] Peter P. Swire & Lauren B. Steinfeld, "Security and Privacy After September 11: The Health Care Example," 86 MINN. L. REV. 1515 (2002). For a more detailed discussion of the intersection of privacy and security, see DEREK E. BAMBAUER, *PRIVACY VERSUS SECURITY*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013). Bambauer's analysis is broadly consistent with the 2002 article and the discussion here.

[15] Id.

[16] Giovanni Buttarelli, "Cybersecurity under the next president: A Symposium with cybersecurity industry leaders; Closing speech at Coalition for Cybersecurity and Law Symposium," (Nov. 16, 2016), at https://edps.europa.eu/sites/default/files/publication/16-11-15_speech_gb_cybersecurity_en.pdf.

[17] Privacy Enhancing Technologies, Data Protection, European Union Agency for Cybersecurity (ENISA), at https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies.

[18] Id.

[19] *See generally* John Selby, *Data Localization Laws: Trade Barrier or Legitimate Responses to*

difficult, we teach our students this first approximation: privacy focuses on who should be authorized to access data, while security focuses on preventing unauthorized access to data. Recognizing that other definitions of privacy can differ, we thus offer *a first definition of "security vs. privacy": A measure designed to increase privacy reduces cybersecurity to the extent the privacy measure increases the risk of unauthorized access.* Suppose, as a hypothetical, that data localization (enacted on the premise that it protects privacy) prevents detection of a cyber-attack or reduces the ability to identify the perpetrator. In that hypothetical, there could be privacy benefits from the localization rule, and there would also be cybersecurity risks resulting from the rule.

Cybersecurity has additional components beyond preventing unauthorized access to data. Cybersecurity traditionally concerns CIA – confidentiality, integrity, and availability. Preventing unauthorized access helps "confidentiality." Measures to ensure "integrity" improve cybersecurity even if the same people are authorized to see the data. One example of protecting integrity is a digital signature, so that people can verify that a communication has not been altered in transit. In addition, measures to ensure "availability" are part of cybersecurity. For instance, measures to address distributed denial of service ("DDOS") attacks are ways to improve availability. If a privacy measure makes it more difficult to resist a DDOS attack, then the stricter privacy protection is accompanied by an increased cybersecurity risk. *More generally, a measure designed to increase privacy reduces cybersecurity to the extent the privacy measure increases the risk of unauthorized access, reduces integrity, or reduces availability.*

It is worth noting that the discussion thus far of the interaction of privacy and cybersecurity is essentially definitional. This explanation makes no empirical claims about the size of effects to improve privacy or reduce cybersecurity. Apart from the size of effects on privacy and cybersecurity, the direction of the effects may be unclear. For instance, multiple back-ups can aid availability (improving cybersecurity) and provide greater assurance that data subjects can access their data (a component of privacy); however, multiple backups also can expand the attack surface, so there may be risks to cybersecurity, potentially greater than the cybersecurity benefits from having redundant backups. Throughout this article, we point out the apparent direction of effects, such as to increase or reduce cybersecurity; we emphasize that identifying an effect in one direction leaves open the possibility that there are simultaneous effects in the other direction, such as the ways that multiple back-ups, all things considered, might either help or hurt cybersecurity.

Cybersecurity Risks, or Both?, 25 INT'L J.L. & INFO. TECH. 213 (2017) (asserting that data localization may enhance cybersecurity and privacy); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015) (discussing several reasons that data localization undermines privacy and cybersecurity); McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643 (2012) (focusing on how the current privacy landscape undermines security by blocking the creation of training datasets required for the development of new security techniques to neutralize new threats); Bruce Schneier, *Security vs. Privacy*, Schneier on Security (Jan. 29, 2008), https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html (emphasizing that describing privacy and security as tradeoffs is a false dichotomy and notes that one does not "have to accept less of one [of privacy or security] to get more of the other").

With that said, we close this discussion of privacy and security by reporting what we found in reviewing a range of official EU discussions of privacy and security. Based on our research, we highlight two points. First, these discussions have provided considerable detail about the areas where privacy and security reinforce each other, such as for encryption and PETs. By contrast, the discussions have provided little detail about how to address topics where the two goals may conflict. Roslyn Layton and Silvia Elaluf-Calderwood, in their extensive study about the EU approach to cybersecurity, concluded the same, saying that GDPR's "significant cyber risks have been downplayed, if not ignored outright."[20] The official EU discussions to date have largely accentuated the positive aspects of the relationship between protecting privacy and cybersecurity. Our research has uncovered almost no discussion of the tension between the two, or even the possibility of effects in both directions. We do not speculate on the reasons why EU discussions have downplayed the tension between privacy and cybersecurity, but the lack of public discussion is striking.

The second point from our review of EU official documents is the legal conclusion that measures to address cybersecurity must be consistent with the protection of the fundamental rights to privacy and data protection. For instance, the European Data Protection Supervisor issued an opinion in 2021 on the EU's cybersecurity strategy and updates to the Network and Information Security Directive.[21] This opinion first reiterated the optimistic view that privacy and security often reinforce each other, and that "improving cybersecurity is essential for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data." It then recognized that pursuing cybersecurity may lead to "deploying measures that interfere with the rights to data protection and privacy of individuals." The EDPS stated that any potential limitation on those rights must meet the strict requirements of Article 52(1) of the EU Charter of Fundamental Rights. That Article notably states that any

---

[20] Roslyn Layton & Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices," IEEE – IEEE Xplore 2019, at https://ieeexplore.ieee.org/abstract/document/8962288.

[21] Opinion on the Cybersecurity Strategy and the NIS 2.0 Directive, EDPS, Mar. 11, 2021, P. 7-8, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en. A similar conclusion appeared in the 2016 EU Directive concerning security of networks and information systems, "This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles." Directive (EU) 2016/1148 (Jul. 6, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1; *see* Dimitra Markopoulou, et al., *The New EU Cybersecurity Framework*, 35 COMPUT. L. & SEC. REV. 1 (2019) (The GDPR will prevail in case of conflict against the EU's Network and Information Security ("NIS") Directive, due to the recognition by Art. 16(2) Treaty on the Functioning of the European Union ("TFEU") that the right to data protection is one of "fundamental EU rights" that can overcome cybersecurity interests.).

limitations on rights must "respect the essence of those rights and freedoms." The Article also provides that any limitations must be "necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." In short, cybersecurity measures under EU law must remain consistent with the requirements of privacy and data protection laws – any potential cybersecurity measure that may reduce privacy protection faces the demanding requirements of Article 52(1).

B. Data Localization for Non-Privacy Reasons

For the EU, the de facto shift toward data localization is driven by legal developments in data protection law, including the *Schrems II* decision and the EDPB Guidance. A range of rationales, in addition to privacy protection, can support data localization. In their review of recent localization measures, Cory and Dascoli write:

> "Nearly all data localization proposals involve mixed motivations. Policymakers often take a "dual-use" approach with an official and seemingly legitimate objective, such as data privacy or cybersecurity, when their primary (hidden) motivation is protectionism, national security, greater control over the Internet, or some combination of these."[22]

Cory and Dascoli discuss a range of objectives for data localization, including data sovereignty, censorship, and implementation of law enforcement and regulatory oversight. For purposes of this paper, we can recognize that diverse reasons might support localization, without needing to assess precisely which reasons actually motivate a particular localization measure. We now turn to discussion of the effects of data localization on cybersecurity, which unless noted do not depend on the rationales for localization.

III. Methodology of the Research

We have used three methods to generate a more systematic understanding of the effects of data localization on cybersecurity: the literature review, the review of approximately 200 public comments to the EDPB, and a step-by-step analysis of the effects of data localization for the controls set forth in an international cybersecurity standard.

The first method is a traditional literature review.[23] A variety of publications have discussed how data localization may affect cybersecurity, often as a paragraph or a few sentences

---

[22] Nigel Cory & Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Fund, July 19, 2021, at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

[23] *See*, *e.g.,* Yantsislav Yanakiev & Todor Tagarev, *Governance Model of a Cybersecurity Network: Best Practices in the Academic Literature*, CompSys Tech (June 2020), at https://dl.acm.org/doi/10.1145/3407982.3407992, ("Proliferating cyber threats, both in terms of diversity and intensity, require a timely development and implementation of effective solutions, which is within the powers of very few organisations, and actually of very few countries. The

in a broader discussion of data localization. For instance, Susan Lund and James Manyika provide the typical arguments from supporters of data localization, including the assurance that the government mandating data localization will have access to data within its territory, the belief that these requirements will create technology jobs in the country, and the desire to protect data of the country's residents from surveillance by foreign governments. As part of this discussion, Lund and Manyika pointed out that cybersecurity experts assert that "the location of a server has no impact on its vulnerability to foreign hackers or government surveillance."[24] When examining whether data localization could be a solution for the EU to address the requirements of the *Schrems II* case, Anupam Chander asserted that data localization created new cybersecurity issues – including a "bigger attack surface for malicious hackers" and slower updates on attackers' information.[25] In addition, to help discover relevant literature and to provide additional insights, we have interviewed on background a number of cybersecurity experts, including senior security engineers in major companies, government officials, and lawyers who specialize in data breaches and international data transfers.

European Union sees collaboration and the establishment of competence networks as indispensable for securing its digital economy, infrastructures, society, and democracy, and preserving its competitive advantages."); P. Sterlini et al., *Governance Challenges for European Cybersecurity Policies: Stakeholder Views*, IEEE Computer and Reliability Societies, January/February 2020, at https://cybersec4europe.eu/wp-content/uploads/2019/11/Governance-Challenges-for-European-CyberSecurity-Policy_-Stakeholders-Views_V.Def_.pdf, ("The EU-wide issue of maintaining a balance between national freedoms and supranational regulations remains problematic because for cyberthreats the distinction between those areas is unclear. From identifying attackers to developing the most efficient responses, cybersecurity increasingly requires intra- and international cooperation as well as cross-domain policy responses."); Josep Domingo-Ferrer, et al., *Technological Challenges in Cybersecurity* (2020) ("National Cyber Defence Strategies" implemented by European countries often lack in-depth description of "concrete countermeasures."); Richard Taylor, *'Data Localization': The Internet in the Balance,* Telecommunications Policy (2020) (While examining the concepts of data sovereignty and transborder data flows, the article notes that at least one country has advocated for democratic governments to focus on cybersecurity threats.), at https://www.sciencedirect.com/science/article/pii/S0308596120300951; David Lore, *Reconciling Data Localization Laws and the Global Flow of Information*, CYBERSECURITY L. REP. (Oct. 11, 2017) (Data localization laws are "designed to ensure access to data for surveillance purposes," by broadly defining national security and creates "redundant data sets that increase the exposure to threats" and creates "distraction of diverse compliance requirements in multiple jurisdictions"); W. Kuan Hon et al., *Policy, Legal, and Regulatory Implications of a Europe-only Cloud*, 24 INT'L J.L. & INFO. TECH. 251 (2016) ("Physical location of data in Europe is not always necessary or sufficient for ensuring that the data will be protected and handled in accordance with European law.").

[24] Susan Lund & James Manyika, *Defending Digital Globalization*, MCKINSEY (Apr. 20, 2017), at https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization#

[25] Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771 (2020).

The second method has been our comprehensive review, published in April, 2021, of the approximately 200 comments submitted in late 2020 to the EDPB on its guidance. Based on a review of all the comments,[26] approximately 25% of the nearly 200 comments submitted to the EDPB expressed concern that the Draft Guidance would result, in practice, in data localization. Slightly more than 10% of the comments spoke explicitly to the concern that the application of the EDPB Draft Guidance would result in data localization, in law, in practice, or both. Nearly an additional 15% of the submissions include language describing similar concepts without using the term data localization – such as return EU commerce and society to a "pre-internet era,"[27] transform the EU into a "digital island," [28] and "balkanize global data flows." [29] Reflecting these comments, the earlier article highlighted five themes:

1. "Many of the effects of the Guidance would have adverse impacts specifically on the EU and its economy.
2. Although not a stated goal, implementation of the Guidance would result in widespread data localization.
3. The Guidance would have negative sector-specific effects.
4. Across sectors, the Guidance would have pervasive, negative effects on current business operations.
5. The Guidance would have broad effects on EU cross-border data flows, entirely apart from the much-discussed data flows between the EU and the US."

Third, for this article we have used standards from the International Standards Organization ("ISO") to provide a step-by-step analysis of the effects of data localization. The best-known ISO cybersecurity standard is ISO/IEC 27001 ("ISO 27001"), last formally issued in 2013. ISO 27001sets forth specifications for an information security management system, providing an overall risk-based framework for managing an organization's cybersecurity. Appendix A to ISO 27001 lists 14 controls to implement in order to meet the standard. These controls are then set forth in more detail in ISO/IEC 27002 ("ISO 27002"), with the title "Information technology — Security techniques — Code of practice for information security

---

[26] DeBrae Kennedy-Mayo & Peter Swire, "Prominent Theme of Data Localization in Comments to EDPB Guidance on Implementing *Schrems II* has New Urgency with the Portuguese Decision," Cross-Border Data Forum (Apr. 29, 2021), at https://www.crossborderdataforum.org/prominent-theme-of-data-localization-in-comments-to-edpb-guidance-on-implementing-schrems-ii-has-new-urgency-with-the-portuguese-decision/#_edn2; *see* Feedback to Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, European Data Protection Board (EDPB), at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en. (Hereinafter, Feedback to Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data will be noted as "comment" followed by the name of the organization providing the feedback.)

[27] Comment by AMETIC (Spain), Comment 12, P. 2; Employers of Poland (Poland); Comment 11, P. 2; Polish Confederation Lewiatan (Poland); Comment 105, P. 1.

[28] Comment by U.S. Chamber of Commerce (U.S.), Comment 63, P. 2-3.

[29] Comment by City of London Law Society (U.K.), Comment 155, P. 6.

controls."[30] In Appendix A, we examine each ISO 27002 control, and its sub-sections, and consider the potential effects of data localization.

This step-by-step analysis of ISO 27002 has assisted our overall understanding in several, related ways. First, the ISO 27002 controls have helped us spot issues not identified in the literature review and EDPB comments. The cybersecurity implications related to auditing is one such issue.[31] With data localization, it is unclear how auditing can occur across the entire system, as it may not be permissible for an asset owner to be in a different jurisdiction than the user. If two countries require data localization, accurate auditing may be unlawful – the data flows out of both countries would be blocked. Another cybersecurity issue we noted is the potential impacts of data localization on logging and monitoring. As to logging, restricted access to IP addresses and other data in a jurisdiction may impact forensic investigations. With regard to monitoring, a recommended intrusion detection system outside of the control of network administrators may be difficult to maintain if localization requires separate sub-systems in an organization's systems.[32] Second, examining each ISO 27002 control increases our confidence that we have identified the principal effects of data localization – ISO 27002 is designed to provide an organized and comprehensive system of controls. Third, perhaps the greatest contribution for our research from ISO 27002 has been to help us identify broader themes for the effects of data localization. *Notably, as discussed further below, many of the ISO 27002 controls emphasize the importance of an organization-wide, rigorous management approach.* Data localization poses many different types of challenges to organization-wide methods for reducing cybersecurity risk.

IV. Categorizing the Effects of Data Localization on Cybersecurity

In the course of our research, we found a confusing jumble of possible effects of data localization on cybersecurity. Some concerns were very technology-specific. For instance, sharding of messages among multiple data centers would no longer be possible across borders.[33] Other concerns were more general. For instance, investigation of cyberattacks in general would become more difficult where data might not be shared with investigators in other nations. As we performed the literature review, and reviewed the comments to the EDPB, the welter of possible

---

[30] Introduction to ISO 27002 (ISO 27002), ISO 27002 Section, The ISO 27000 Directory, https://www.27000.org/iso-27002.htm.

[31] ISO 27002 Controls: 12.7 - Information systems audit considerations; *see* 8 - Asset Management; 9.25 – Review of User Access Rights; 12.6 - Technical Vulnerability Management, https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf; *see generally* Peter Swire & Robert Litan, NONE OF YOUR BUSINESS, Chapter 5, Section B – Auditing and Accounting.

[32] ISO 27002 Controls: 12.4 - Logging and Monitoring; *see* 12.4.3 – Administrator and Operator Logs.

[33] *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015) ("Requirements to localize data . . . only make it impossible for cloud service providers to take advantage of the Internet's distributed infrastructure and use sharding and obfuscation on a global scale") (*quoting* Patrick Ryan, et al., *When the Cloud Goes Local: The Global Problem with Data Localization*, COMPUT., Dec. 2013, at 54, 56).

effects remained confusing. By contrast, once we worked through the 14 controls in ISO 27002, a clearer pattern started to emerge, which we present for the readers' consideration.

We are now prepared to propose a way to organize the effects of data localization rules on cybersecurity. First, *data localization creates obstacles to integrated management of cybersecurity risk within a single organization,* such as a corporation or government agency. Second, data localization creates obstacles for an organization in using *cybersecurity-related services* from outside of the organization. Third, apart from cybersecurity services, data localization creates obstacles to *information sharing* between organizations, and information sharing is an important tool for reducing cybersecurity risk.

In considering the effects of data localization, we explained above reasons why a strategy may succeed of consolidating data in one region, such as the EU, if only one country or region requires localization. If India then also requires localization, however, then the data cannot all be sent to the EU and to India. When more than two countries or regions require localization, the complexity and potential effects on cybersecurity grow further – an organization then needs to segregate its network in an increasing variety of ways, depending on nation and type of data. As more countries create localization limits, organizations also will face more conflicts of law – situations where one country says data must be transferred to that country (such as for accounting or regulatory oversight), and another country says the transfer is unlawful. In this event of a globally fractured Internet, the impact of data localization on cybersecurity becomes systemic (as opposed to incidental) as the cost and complexity of managing global systems and risks becomes significant.

A. Not Assessing Current Legal Prohibitions on Data Transfers

Before providing more detail on these three categories, we provide a disclaimer about legal conclusions in this paper. The topic of the paper is to describe effects on cybersecurity, *if and when* a nation creates de jure or de facto data localization. This paper does not seek to make legal conclusions about which national laws prohibit which categories of data flows.

The task of this paper is to assess the effects of hard data localization, where transfers of a category of data are prohibited to the other country. In practice, countries may draft exceptions to data localization rules. For instance, consider the possibility that a company has its best cybersecurity experts living in one country, such as the U.S., but provides services in different countries, which have localization rules. If there is a strict localization rule, then it would no longer be lawful to elevate cybersecurity problems to experts living in the U.S. in situations where those experts would have access to the data. However, countries with localization rules could make an exception, permitting escalation to experts in the U.S. when local personnel cannot solve the problem. The example illustrates another possible contribution from this paper. Most of the paper analyzes the cybersecurity risks created by localization; instead, the analysis in

this paper could help identify situations where a country with localization rules might wish to consider an exception, such as the escalation exception.[34]

With that said, we discuss the European Union and India as two important geographies that have recently increased limits on data transfers. For India, localization is already required for financial transactions, and broader rules for localization may result from new privacy legislation. For the EU, after *Schrems II* and the EDPB guidance, there has a been a growing number of enforcement actions against data transfers, and legal uncertainty may chill the willingness of organizations in the EU to transfer data to third countries. In addition, the legal standard for processing personal data within the EU is easier to meet than the legal standard for transferring such data to another country that lacks an adequacy decision.[35] For ease of exposition, we use examples from the EU and India below, to the extent limits on data transfers exist.

B. Obstacles to Integrated Management of Cybersecurity Due to Data Localization.

In order to explain the obstacles to integrated management arising from data localization, we first show obstacles to fulfilling the ISO 27002 controls. We next provide examples from the comments to the EDPB of ways that data localization creates obstacles to integrated management.

1. ISO 27002 Controls

Review of the ISO 27002 controls shows the pervasive effect that data localization would have on the ability of an organization to achieve integrated management of cybersecurity risk. In Appendix A, we provide discussion for each relevant section of ISO 27002, as well as multiple sub-sections. Appendix A examines effects of a localization rule that prohibits transfer of personal data, although the analogous analysis can be made for other types of localization rules. We find that 13 of the 14 controls, as well as numerous sub-controls, can be affected when globalized management of data shifts to management of segregated national systems. As shown in detail in the Appendix, the shift away from globalized management affects:

- Control 5, policies for information security;

[34] An exception of this sort might be narrow, such as the exception described in text for escalation. Alternatively, an exception may be broader, such as if the transfer is "necessary" to protect cybersecurity, and the scope of the transfer is proportionate to that need.

[35] Our understanding is that the legal standard for processing cybersecurity-related personal data would be covered by Recital 49 GDPR, which states that processing for purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned under Art. 6 GDPR. This legitimate basis test for processing data within the EU is less strict than for transfers to a non-adequate country, such as the U.S. Compelling legitimate interest is one derogation (exception) for transferring data under Article 49(1) GDPR, but the exception is accompanied by a series of additional requirements. For instance, the transferring company would have the obligation to inform the relevant supervisory authority of the anticipated transfer, which in practice companies may be reluctant to do.

- Control 6, organization, including specification of roles;
- Control 7, human resource security;
- Control 8, asset management;
- Control 9, access control;
- Control 12, operations security;
- Control 13, communications security;
- Control 14, system acquisition, development and maintenance;
- Control 15, supplier relationships;
- Control 16, information security management;
- Control 17, information security aspects of business continuity management; and
- Control 18, compliance.

The one control missing from this list is Control 11, physical and environmental security, which is often managed locally.

The only other control in ISO 27002 is cryptography, where encryption algorithms, and implementing crypto-systems, may not themselves require transfers of personal data. On the other hand, because the organization for compliance purposes may need to prove that personal data has not been transferred illegally, a data localization rule may be inconsistent with the use of end-to-end ("E2E") encryption – the localization rule may require the organization to have a technique for logging what content is transferred, or at least to have a mechanism to do forensics in case of concern about an illegal transfer.

2. Examples of Obstacles to Integrated Management

Appendix A chronicles the numerous ways that a localization rule creates obstacles to integrated management of an organization's cybersecurity. *One general result of localization is greater complexity*, to manage the network segregated by nation, and "complexity is the enemy of cybersecurity."[36] *Another general result is to reduce the ability of the organization to benefit from an efficient division of labor.* For a globalized organization network, individuals with specialized skills might live and work in one or a few countries; with localization, those same functions may need to be performed in each country with a localization regime. The result for the organization would be a mix of hiring previously unneeded employees or using existing employees to manage functions that had previously been handled by experts in a different jurisdiction. Small and mid-sized enterprises (SMEs) are likely to encounter disproportionate difficulties in dealing with these issues.

In addition to the list of effects on integrated management in Appendix A, we highlight some effects published in comments on the November, 2020 EDPB Guidance. These effects could result, for instance, from limits on transfers of personal data from the EU to third countries that lack an adequacy determination.

[36] VMWare Editorial Board, "Complexity Is the Enemy of Security: VMware Leaders Weigh In On How To Make Security Simpler, Faster and Smarter," VMWare Security & Compliance Blog (June 29, 2021), at https://blogs.vmware.com/security/2021/06/complexity-is-the-enemy-of-security-vmware-leaders-weigh-in-on-how-to-make-security-simpler-faster-and-smarter.html.

1. Human resources. Localization could limit transfer of employee data in a wide range of settings, including affecting business operations that ensure European employees get paid on time.[37]
2. Customer/user support. Many global organizations offer customer support through a "follow the sun' model, such as having support centers in Europe, Asia, and North America.[38] On-call engineering teams worldwide can be used to constantly monitor cybersecurity issues.[39] A maintenance team of specialists may exist in one country, such as the U.S.[40] These support services would be blocked to the extent data would no longer be permitted to go abroad.
3. Audit and compliance. Localization makes it difficult to document and ensure compliance with diverse national laws,[41] and makes it unclear the extent to which organization-wide audits can be performed.[42]
4. Encryption may be affected, such as when it would prevent proof of compliance with rules against transferring data.[43]
5. Sharding. Localization prohibits "sharding," in instances where some of a stored record is stored in pieces in more than one nation.[44]
6. Integrated management generally. The comments cited a variety of ways in which integrated management of an organization's cybersecurity would be more difficult, including resilience,[45] creating a single point of failure,[46] anti-virus checking for attachments,[47] redundancy and backups,[48] and authentication.[49]

In sum, data localization would appear have numerous, sometimes-overlapping effects on the ability of an organization to operate an integrated program to manage cybersecurity risk.

3. Possible benefits of localization and mitigation of risks.

Our discussion thus far has examined risks to cybersecurity from data localization. We next examine the principal arguments we have seen for why localization may improve cybersecurity, to protect privacy (the security of personal data), further "data sovereignty," and

[37] Comments by Software and Information Industry Association; TechNet, techUK.
[38] Comments by Confederation of Finnish Industries EK; Global Data Alliance.
[39] Comment by Global Data Alliance.
[40] Comment by Adigital.
[41] Comment by Workday, Inc.
[42] Comment by Workday, Inc.
[43] Comments by American Chamber of Commerce-Ireland; American Chamber of Commerce in Spain; Asia Cloud Computing Association; Information Technology Industry Council; tech UK, U.S. Mission to the EU.
[44] Comment by Information Technology Industry Council.
[45] Comments by Information Technology Industry Council; Palo Alto Networks.
[46] Comment by Information Technology Industry Council; Palo Alto Networks.
[47] Comment by Polish Chamber of Information Technology and Communications.
[48] Comment by Peter Swire & DeBrae Kennedy-Mayo.
[49] Comment by Polish Chamber of Information Technology and Communications.

uphold national security. We then examine how such arguments may vary by the size of the localization area.

Perhaps the most common argument for data localization, within democracies that regulate to protect privacy, is to assure a high level of protection of data held within the country. As Théodore Christakis has written, "European calls in favor of data localisation are often motivated by genuine and legitimate concerns, related to data protection, privacy considerations and the fear of foreign snooping into European personal and industrial data."[50] The discussion above addressed the interactions of data protection and privacy with cybersecurity. A somewhat broader point is the concern in general for "foreign snooping," the idea that a hostile nation, or even allied nation such as the U.S., might create harm by examining the data.

The second argument for data localization, used in both democratic and non-democratic nations, is the issue of "data sovereignty." In Christakis' magisterial study of European data sovereignty, he says the term "is an extremely powerful concept, broad and ambiguous enough to encompass very different things and to become a 'projection surface for a wide variety of political demands.'"[51] Christakis first analyzes data sovereignty as "regulatory power," concerning the ability of the EU or its Member States to enact effective regulations, such as to protect privacy. He then analyzes data sovereignty as "strategic autonomy," which is "the ability to act in the digital sphere without being restricted to an undesired extent by external dependencies."

In assessing data localization, such as increasingly exists as a matter of fact for the EU, there will thus be potential benefits from localization (such as privacy protection and strategic autonomy) as well as potential risks, including the obstacles to integrated cybersecurity management discussed above. Christakis proposes an approach that we find both persuasive and consistent with general principles of European law: "[T]he critical test should be whether restrictions to transnational data flows are proportionate to the risks presented, taking into account the nature of the data and a series of other considerations." Christakis would find data localization to be a disproportionate or unnecessary response "where the likelihood of foreign access to data is very limited and where other, more satisfactory and less disruptive, solutions exist." In our concluding discussion, we return to the test proposed by Christakis, to examine net effects of data localization on cybersecurity.

---

[50] Christakis, Theodore and Christakis, Theodore, 'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy (December 7, 2020), at https://ssrn.com/abstract=3748098 or http://dx.doi.org/10.2139/ssrn.3748098; *see* "Data localization provides better information security against foreign intelligence agencies." John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both," International Journal of Law and Information Technology, Volume 25, Issue 3, Autumn 207, pp. 213-232, ("Data localization provides better information security against foreign intelligence agencies.") at https://academic.oup.com/ijlit/article/25/3/213/3960261.

[51] Id.

Next, non-democratic countries concern for data leaving the country appears to focus less on the protections for the data of individuals and more on national security implications.[52] China's requirement of a national security review of data that leaves the country is an example.[53] A second concern in non-democratic countries who have data localization requirements relates to

[52] *See* Jyh-An Lee, Hacking into China's Cybersecurity Law, 53 WAKE FOREST L. REV. 57, 90 (2018) (stating that, in socialist countries, the focus in cybersecurity is political threats); Rogier Creemers, *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-Firs Century*, 26 J. CONTEMP. CHINA 85, 95 (2017) (arguing that China's Internet governance as designed to maintain the stability of the regime); *see generally* Ngoc Son Bui, CONSTITUTIONAL CHANGE IN THE CONTEMPORARY SOCIALIST WORLD (Oxford 2020), at https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198851349.001.0001/oso-9780198851349. See *See* Anupam Chander and Uyen Le, "Data Nationalism," 64 Emory L. R. 677 (2015) (discussing different motivations of democratic and non-democratic regimes), https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/.

[53] Both the Data Security Law (DSL) and the Cybersecurity Law in China focus on two areas: "efforts to protect data security" and to "regulate cross-border data transfers. … The DSL establishes a data security review regime to identify data processing activities that impact or may impact national security. … [I]ndividuals and organizations are expressly prohibited under the DSL from providing data stored in China to foreign law enforcement authorities, save with the prior approval of relevant Chinese authorities." Akin Gump, "Impact of the New China Data Security Law for International Investors and Businesses," Asia Alert (July 26, 2021), at https://www.akingump.com/en/news-insights/impact-of-the-new-china-data-security-law-for-businesses-and-international-investors-1.html. "With data viewed as a 'national basic strategic resource', an increasing number of Asian countries – mainly, but not exclusively, China, Indonesia and Vietnam – have adopted, or are considering laws requiring that data generated locally on their citizens and residents be kept within their geographic boundaries and remain subject to local laws. The protection of privacy and national security interests, aid to law enforcement, and preventing foreign surveillance, in addition to appeals to the principle of sovereignty, are the classic motives supporting such measures." Clarisse Girot (editor), "Regulation of Cross-Border Data Transfers of Personal Data in Asia, Asian Business Law Institute (ABLI), May 28, 2018, p. 16, at https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia.

data entering the country. These countries typically restrict the data that citizens can access.[54] The best-known example of this approach is the Great Firewall of China.[55]

In addition to these general considerations possibly supporting localization – protecting privacy, data sovereignty, and national security – the risks and benefits would appear to vary considerably based on the size of the localized market. Consider the possibility of sharding among multiple data centers or providing physically separate data centers for backup purposes. Large markets such as China may reach efficient scale for these security controls.[56] By contrast, smaller countries may not be large enough to support even one world-class data center, much less provide an economic rationale for multiple data centers, which can cost a billion dollars or more.[57]

C. Limitations on Cybersecurity-Related Services by Third Parties

In addition to internal management of cybersecurity risk, a large and growing fraction of organizations now use third parties to address cybersecurity risk. The discussion here first defines the cybersecurity services markets, which are enormous and growing quickly. It analyzes what players would be affected by localization. For instance, localization would adversely affect both large and small purchasers of cybersecurity services, as well as both large and small service providers. The discussion then shows specific examples of effects on cybersecurity services, drawn from the EDPB comments.

---

[54] "[C]ertain countries have a much broader vision of exercising greater control over all activities in domestic cyberspace through data localization, including the information available to its citizens." Neha Mishra, "Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?" World Trade Review, Volume 19, Issue 3, July 2020, pp. 341-364, at https://www.cambridge.org/core/journals/world-trade-review/article/privacy-cybersecurity-and-gats-article-xiv-a-new-frontier-for-trade-and-internet-regulation/F46D255A399C0A30B9BA68021EC28947; *see* Geoffrey Hoffman, *Cybersecurity Norm-Building and Signaling with China*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 187, 189 (explaining how China uses censorship for its approach to cybersecurity).

[55] Jyh-An Lee and Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J. L. SCI. & TECH. 125, 129-135 (2012); Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 55-56 (2019).

[56] "The protections claimed by Chander and Le to be offered by 'sharding' data would still be possible if a country as large as Brazil, Russia, India or China built multiple local data centres." John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both," International Journal of Law and Information Technology, Volume 25, Issue 3, Autumn 207, pp. 213-232, at https://academic.oup.com/ijlit/article/25/3/213/3960261.

[57] Rich Miller, "The Billion-Dollar Data Centers," Data Center Knowledge, (Apr. 29, 2013), https://www.datacenterknowledge.com/archives/2013/04/29/the-billion-dollar-data-centers

1. Defining the Cybersecurity Services Markets

Definitions vary for categories of third-party services. A variety of terms is used to describe these services, including cloud computing, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).[58] Vendors and experts differ on precisely what is covered by each category, but the definitions by Watts and Raza give a sense of the differences. They say: "SaaS utilizes the internet to deliver applications, which are managed by a third-party vendor, to its users. A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side."[59] Next, "Cloud platform services, also known as Platform as a Service (PaaS), provide cloud components to certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications."[60] In addition, "IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services."[61] That is, IaaS clients retain "complete control over the entire infrastructure."[62] These definitions of SaaS, PaaS, and IaaS suggest the range of ways that organizations rely on third parties services, including for software that addresses cybersecurity.

The size of the market for such services is enormous and growing, although once again definitions vary for what fits within the cybersecurity or information security sectors. Estimated spending in 2021 for cybersecurity services is roughly $200 billion,[63] and expected to grow to roughly $350-400 billion by 2027.[64] To the extent data localization impacts the provision of cybersecurity-related services, localization would affect this very large sector.

---

[58] Stephen Watts & Muhammed Raza, "SaaS vs PaaS vs IaaS: What's The Difference & How To Choose," BMC blogs (June 15, 2019), at https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose.

[59] Id.

[60] Id.

[61] Id.

[62] Id.

[63] "Cyber Security market is projected to grow from USD 165.78 billion in 2021 to USD 366.10 billion in 2028 at a CAGR of 12.0% during the 2021-2028 period." Cyber Security Market Size, Share & COVID-19 Impact Analysis, 2021-2028, Fortune Business Insights, March 2021, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165. The size of the cybersecurity market in 2021 was $217.9 billion. "Size of the Cybersecurity Market Worldwide, from 2021 to 2026 (in Billion U.S. Dollard), Technology & Telecommunications, IT Services, Statista, https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/.

[64] Global Market Insights, "Cybersecurity Market to Hit $400 Billion by 2027: Global Marketing Insights, Inc.," CISION (June 29, 2021), at https://www.prnewswire.com/news-releases/cybersecurity-market-size-to-hit-400-bn-by-2027-global-market-insights-inc-301321491.html; Size of the Cybersecurity Market Worldwide, from 2021 to 2026 (in Billion U.S. Dollard), Technology & Telecommunications, IT Services, Statista, https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/.

The effect of localization is greater because one country, *the United States, has been by far the market leader to date* for cloud computing generally and cybersecurity services more narrowly defined.[65] Among cloud providers, the top three are Amazon, Google, and Microsoft, with eight of the ten largest providers based in the U.S., along with one each from China (Alibaba) and Europe (SAP).[66] One study of specialized cybersecurity vendors, excluding the cloud providers, listed the market shares of the top eight companies, all of which are based in the U.S.[67] Any prohibition on cybersecurity services from the U.S. would thus greatly affect current deployment of cybersecurity services.[68]

The effect of localization is also greater because *third-party service providers often access a wide range of data* within the client organization. For example, intrusion detection services report granular details to the service provider. Many security services access IP logs, revealing personal data about those who interacted with the company. Forensics firms need to dig deep to detect the nature and scope of breaches. More generally, cybersecurity services, in order to do their job, often need privileges similar to those of the organization's systems

---

[65] For example, Guillaume Poupard, director of France's ANSSI – the country's cybersecurity agency, has spoken on the topic of developing cybersecurity services within the EU. According to Politico, "[If] Poupard has his way, new EU rules would prevent critical data from ending up with U.S. authorities. The rule "would exclude the standard American and Chinese services" from offering services in critical sectors in Europe, said Poupard. … European governments are trying to grow less dependent on U.S. cloud services as part of their drive toward 'strategic autonomy,' the idea that Europe needs to keep control over technology policy, in part due to fears of spying and surveillance from the U.S. The new cloud cybersecurity rule "will be a real test, a real objective for the political will to achieve strategic autonomy in the digital field,' Poupard said. 'If we're not capable to say this, the notion of European sovereignty doesn't make sense.'" Laurens Cerulus, "France Wants Cyber Rule to Curb US Access to EU Data," Politico, September 13, 2021, at https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/; *see* Aaron Raj, "In Europe, Big Tech Providers are at the Mercy of Data Sovereignty," TechHQ, October 12, 2021, at https://techhq.com/2021/10/in-europe-big-tech-providers-are-at-the-mercy-of-data-sovereignty/ (discussing France's sovereign cloud which will manage cybersecurity issues).

[66] Shelby Hiter, "Cloud Computing Market 2021, August 13, 2021, https://www.datamation.com/cloud/cloud-computing-market/. As noted in the first footnote, research support for this paper has come from Microsoft, a cloud provider, and from the Cross-Border Data Forum, whose financial supporters include major cloud providers. All statements in this paper, as noted there, are those of the authors alone.

[67] "Leading Cybersecurity Vendors by Market Share Worldwide from 2017 to 2020," Technology & Telecommunications, Software, Statista, at https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share/.

[68] "The Protected Local Provider offering storage and processing services may be more likely to have weak security infrastructure than companies that continuously improve their security to respond to the ever-growing sophistication of cyberthieves." Anupam Chander and Uyen Le, "Data Nationalism," 64 Emory L. R. 677, 719 (2015), at https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=elj.

administrators. Due to the broad and deep access by service providers, many sorts of data localization rules could prohibit use of foreign cybersecurity providers – localization may affect not only personal data in the EU, but the many different categories of data reported in the Cory and Dascoli study.

Localization rules would affect both large and small purchasers of cybersecurity services. The dependence of large organizations on cybersecurity services was underscored by the SolarWinds attacks in 2019 and 2020 – U.S. government agencies and major corporations were users of the SolarWinds cybersecurity services. Large organizations have led in the adoption of cloud computing and cybersecurity services. Given their size, management understands that they are likely to be a target, and many large organizations are part of critical infrastructure, where attacks can cause greater harm and where advanced persistent threats are more likely to strike. On the other hand, small and medium enterprises ("SMEs") also have important and increasing reason to seek assistance from third-party service providers. With a shortage of cybersecurity experts and limited budgets, SME's often lack the in-house capability to implement and update high-quality cybersecurity measures.[69] The epidemic of ransomware attacks against small municipalities and other smaller organizations is evidence of the need for SME's to get third-party assistance to manage cybersecurity.[70] Thus, the impact is disproportionate as SME's do not have the same resources to recruit, hire, train, and retain relevant cybersecurity expertise in comparison to large multinationals.

Localization rules clearly affect small providers of cybersecurity services, such as those with headquarters and cybersecurity operations in one country. In the absence of localization, many cybersecurity start-ups have attracted venture capital and sold their services internationally. With data localization, smaller cybersecurity enterprises may not receive funding, and often may find that it is not worth providing service to a country with localization rules.

Large providers, however, also face important costs and challenges to comply with localization. First, with the proliferation of localization laws, it would become more common for data to be required to be stored in one place (such as the EU) and also another country (such as India), but with transfers and data sharing prohibited. That is, there may be no lawful way to

[69] Cyber Security Market Size, Share & COVID-19 Impact Analysis, 2021-2028, Fortune Business Insights, March 2021, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

[70] *See* Andy Castillo, "Ransomware Attacks Highlight Need for Adequate Cybersecurity," American City & County (Jul. 7, 2021), https://www.americancityandcounty.com/2021/07/07/ransomware-attacks-highlight-need-for-adequate-cybersecurity/; Lisa Thompson & Hage Hodes, "Practical Measures for Local Government to Avoid Ransomware," ICMA Blog (Jun. 4, 2021), https://icma.org/blog-posts/practical-measures-local-government-avoid-ransomware; Alison DeNisco Rayome, "Why SMBs are at High Risk for Ransomware Attacks, and How They Can Protect Themselves," TechRepublic (May 8, 2017), https://www.techrepublic.com/article/why-smbs-are-at-high-risk-for-ransomware-attacks-and-how-they-can-protect-themselves/.

comply with both regimes, and large companies may be early targets for enforcement actions.[71] Second, service providers may increase their capacity to serve major regions, such as the EU and India, with many hundreds of million people. For smaller countries, even for large service providers, it may no longer be economic to provide service locally. Third, even large companies may no longer be able to provide 24/7 service if they have to stop using a "follow the sun" strategy for staffing service activities. Fourth, for cutting-edge cybersecurity services, even the largest providers may have only one or a few geographies where their most sophisticated cyber experts live. When difficult issues get elevated to a company's top experts, those experts will only be in those limited geographies, and so may not be able to assist clients in other countries.

2. Examples of Risks to Cybersecurity Services Due to Data Localization

No matter the type of service, there are general possible effects from a limit on out-of-jurisdiction cybersecurity services.

Localization would cut a country off from the state-of-the-art in cybersecurity defense. Organizations within the jurisdiction would need to do the cybersecurity work in-house or purchase services only from permitted jurisdictions. Without access to cutting-edge services, organizations in the localizing jurisdiction would have weaker cybersecurity defenses. Updates and patches may be available more slowly. In addition, attackers would know that the jurisdiction lacked access to state-of-the-art services; that knowledge would provide an incentive for attackers to flock to a jurisdiction that lacked the best security.

The obstacles to integrated management would apply to third-party services as well. The discussion above showed how data localization creates numerous obstacles to an organization integrating its own management of cybersecurity risk. The implicit assumption above was that the organization was doing this work in-house. In fact, organizations operating in more than one country pervasively hire third-party service providers, and these providers would encounter the same obstacles in seeking to assist the organization achieve integrated management. For instance, an organization might hire a third-party service to provide "follow the sun" customer service or cybersecurity management; those third-party services would face the same legal barriers as providing such services in-house.

Localization would reduce innovation in cybersecurity services. In recent years there have been numerous start-ups and other sources of innovation in cybersecurity services. Investment in such innovations has been based on a large international market for such services. If there is substantial localization, investors will face a smaller expected market for any given innovation, and the level of investment and innovation will fall, at a time when government leaders and cybersecurity experts are calling for greater innovation and progress in cybersecurity defenses.

[71] Peter Swire, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," 32 *The International Lawyer* 991 (1998) (large companies analogized to "elephants," who cannot easily hide from enforcers).

The comments to the EDPB analyzed effects of localization on third-party cybersecurity services:

1. State-of-the-art cybersecurity services.[72]
2. Global cloud service providers.[73]
3. Global supply chains.[74]
4. Information security talent outside of the Single Market.[75]
5. Resolution of bugs or security issues in relation to personal data hosted.[76]
6. Packet inspection.[77]
7. Monitoring for cyber threats.[78]
8. Threat intelligence and threat prevention.[79]

3. Possible Benefits of Localization and Mitigation of Its Risks

Along with the risks from cutting off foreign cybersecurity-related services, proponents of data localization have cited the growth of cybersecurity services "closer to home" as a reason to support localization.[80]

We offer three reasons to doubt that the benefits of home-grown cybersecurity services exceed the risks. First, there would appear to be substantial short- to medium-term risks when a country prohibits its industry and individuals from purchasing world-class cybersecurity services. Until the domestic industry is well established, it would appear that attackers would know that the most advanced services are no longer permitted in the country. That is, attackers would rationally target the country that has prohibited the best services. Second, the ability to foster high-quality domestic services would vary greatly depending on the size and sophistication of the localized region. For instance, the largest economies might provide enough scale and

[72] Comments by AmCham Czech Republic; Polish Confederation Lewiatan; SAPIE.
[73] Comments by American Chamber of Commerce in Spain; BAS The Software Alliance.
[74] Comments by Vodaphone.
[75] Comment by U.S. Chamber of Commerce.
[76] Comment by European Organization for Research and Treatment of Cancer.
[77] Comments by American Chamber of Commerce in Slovenia; BSA The Software Alliance; Confederation of Industry in the Czech Republic; Confederation of Swedish Enterprise; Information Technology Industry Council.
[78] Comment by Palo Alto Networks. We note that such monitoring may exist as a service; such monitoring may also exist outside of the services sector, as an example of information sharing as discussed below.
[79] Comments by Palo Alto Networks; Software and Information Industry Association.
[80] "Many governments believe that by forcing companies to localize data within national borders, they will increase investment at home." Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 721 (2015). Countries engaged in "data localization might be able to tap into those local repositories of talent to improve the cybersecurity of their local data centres." John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both," International Journal of Law and Information Technology, Volume 25, Issue 3, Autumn 207, at https://academic.oup.com/ijlit/article/25/3/213/3960261.

local expertise sufficient over time to create competitive cybersecurity services. For smaller countries, however, it is difficult to see how they could hope to provide domestic cybersecurity that come close to the best in the world. Third, in a global market of roughly $200 billion, there are innumerable niche markets in cybersecurity. It will be extremely challenging for most countries to reproduce the same diversity of niche services domestically. Where those niche services do not develop effectively, the country will have greater vulnerabilities than countries that enable access to best-in-class services from other markets.

D. Obstacles to Information Sharing.

A mantra in cybersecurity policy discussions has often been that there should be more information sharing.[81] One obvious effect of data localization is to reduce information sharing across borders, for the scope of data covered by the localization requirement. The discussion here first examines when information sharing is likely to support better cybersecurity (and privacy), and then looks at examples of information sharing that might be interrupted by localization rules.

As a definitional matter, the two categories of cybersecurity services and information sharing are intended to cover the full range of cybersecurity effects involving third parties. An organization might purchase services to improve cybersecurity. As a complement, it might share information to reduce cybersecurity risk, without the purchase of services.

1. Understanding Information Sharing, Cybersecurity, and Privacy.

For one of the authors (Swire), the topic of information sharing, cybersecurity, and privacy has been the subject of two previous research projects, one of which focused on information sharing and cybersecurity, and the other on information sharing effects on both cybersecurity and privacy. The discussion here highlights the relevant points for data localization.

The first paper focused on cybersecurity: "A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?"[82] The paper asked the question of when disclosure (information sharing) helps or hurts cybersecurity. A paradox is that many cybersecurity experts, especially in the Open Source community, favor disclosure and say "there

[81] *E.g.*, Steven Norton, "Former NSA Director: Better Information Sharing Needed on Cybersecurity," Wall Street Journal, Sept. 30, 2014, (Gen. Keith Alexander saying "We need real-time or near real-time situational awareness, and we have got to have cyber legislation that allows us to go between industry and government to do that."), at https://www.wsj.com/articles/BL-CIOB-5467.

[82] Peter Swire, "A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?" 3 *J. Telecomm. & High Technology L.* 163 (2004); republished in Knowledge Policy for the 21st Century (Mark Perry & Brian Fitzgerald, eds.) (2009). The model was extended in another paper, Peter Swire "A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems," 42 *Houston Law Review* 1333 (2006).

is no security through obscurity." On the other hand, military wisdom states that "loose lips sink ships," because disclosure can harm security. The article offers a model for when each is true. For purposes of data localization, the Open Source approach is more valid to the extent three things are true: (1) disclosure will offer little or no help to attackers; (2) disclosure will tend to upgrade the design of defenses; and (3) disclosure will spread effective defenses to more organizations.

In essence, information sharing helps cybersecurity where the benefits of disclosure to the defenders are greater than the risks of disclosure to the attackers. These conditions are often true, such as when a vulnerability is being used by attackers (is known to attackers) and cybersecurity would benefit if more defenders learn about the problem. The discussion below provides more examples.

The second paper analyzed information sharing in the period after the attacks of September 11, 2001. At that time, policymakers often called for a major shift in philosophy from the old "need to know" approach for intelligence and other government actions to a new culture of "need to share." The article, entitled "Privacy and Information Sharing in the War Against Terrorism,"[83] accepted the need to share information in a wide number of settings. It then asked "which information should be shared, with whom and under what circumstances." The article proposed a "Due Diligence Checklist for a Proposed Information Sharing Program." Written during the post 9/11enthusiasm for more data sharing, the ten items were designed to help instill rigor before assuming that information sharing would be beneficial:

1. "Will the proposed sharing tip off adversaries?
2. Does the proposal improve security? Cost-effectively?
3. Is the proposal "security theater"? How much does it provide only the appearance of security?
4. Are there novel aspects to the proposed surveillance and sharing? What risks, if any, accompany these novel aspects?
5. Are there relevant lessons from historical instances of abuse? What checks and balances would mitigate risks of such abuse?
6. Do fairness and anti-discrimination concerns reduce the desirability of the proposed program?
7. Are there ways that the proposed measure could make the security problems worse?
8. What are the ramifications internationally and with other stakeholders?
9. Are there additional, privacy-based harms from the proposed measure?
10. Will bad publicity undermine the program?"

Taking the two papers together, the mantra of improving cybersecurity through information sharing will often be true. In such instances, localization rules will reduce cybersecurity. Such findings, however, are subject to the constraints discussed in the two earlier papers.

[83] Peter Swire, "Privacy and Information Sharing in the War on Terrorism," 51 *Villanova L. Rev.* 260 (2006).

2. Examples of Cybersecurity Risks for Information Sharing Due to Data Localization

A pervasive tool in cybersecurity is to share information with other parties, in order to improve defense. The importance of information sharing has led to important institutions such as CERTs (computer emergency response teams) and ISACs (information sharing and analysis centers), and to new laws designed to enhance information sharing such as the Cybersecurity Information Sharing Act of 2015. *When data localization blocks information sharing, it poses risk to the effectiveness of many established and possible future institutional methods for information sharing.* In the case of CERTs, it also acts as an example of non-reciprocal cooperation in that a CERT in India, for example, may be precluded from sharing data, yet still benefits from information shared from other countries without data localization.[84]

As discussed above, important cybersecurity services include services that monitor for cyberattacks and provide threat analysis and threat prevention. These services often include significant information sharing, such as information about IP addresses associated with cyberattacks. Many cybersecurity services, that is, incorporate information sharing among different organizations; *obstacles to international provision of such cybersecurity services are also obstacles to information sharing.*

Drawing on the comments to the EDPB, data localization poses risk to at least these important categories of information sharing:

1. *Investigation of serious crimes,* including cybercrime.[85] Because such a large portion of cyberattacks originate in a different country, limits on information sharing affect the ability to cooperate on investigation of cyberattacks. More generally, cloud computing has led to the "globalization of criminal evidence" [86] – investigation of crimes other than cybercrime are also often limited if data cannot be transferred from another country.

[84] "[Data localization] prevents the sharing of data to identify IT system vulnerabilities and help firms detect and respond to cyberattacks. For example, in 2020, India's Securities and Exchange Board released a cybersecurity circular that requires financial firms to localize a broad range of data that would do just this." Nigel Cory & Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology & Innovation Fund, July 19, 2021, at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost; *see* The Security and Exchange Board of India, "Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions," November 3, 2020, at https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html.

[85] Comments by Center for Information Policy Leadership; CrowdStrike, Interactive Advertising Bureau Poland; Software and Information Industry Association; U.S. Mission to the EU.

[86] Jennifer Daskal, Peter Swire & Théodore Christakis, "The Globalization of Criminal Evidence," IAPP Privacy Tracker, (Oct. 16, 2018), at https://iapp.org/news/a/the-globalization-of-criminal-evidence/.

2. *Forensic investigations of cyberattacks*, including DDOS, malware, phishing, and ransomware.[87] Investigation of breaches and other cyberattacks often requires extensive forensic investigation. Because attackers often intentionally hop among different countries to avoid detection, forensic investigations can become much less effective in the absence of information sharing across borders.
3. *Global training of datasets.*[88] Cybersecurity increasingly relies on machine learning, artificial intelligence, and other automated techniques to detect and respond to cyberattacks. Data localization reduces the range of data available, in any one country, to train datasets for such defensive measures. In addition, data localization prevents detection of potentially useful patterns, where such patterns can only be detected using data from multiple countries.
4. *Anti-fraud.*[89] Information is pervasively shared to reduce the incidence and costs of fraud. A familiar example to many people is when they receive an alert about an out-of-pattern purchase for their credit card. In such instance, the bank or service provider has accumulated enough information about purchasing patterns to detect what is out-of-pattern. Electronic commerce sites, insurance companies, financial services firms generally, and many other sectors rely on information sharing to reduce fraud. Data localization cuts off information sharing used in fraud detection and prevention, allowing greater criminal activity, both online and more generally.

In sum, on information sharing, data localization creates risk for this pervasive category of cybersecurity defense.

3. Possible Benefits of Localization and Mitigation of Its Risks

[87] Comments by CrowdStrike; Palo Alto Networks. In 2021, 30 countries entered into an international ransomware information sharing initiative. The countries are: Australia, Brazil, Bulgaria, Canada, Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States. "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021, The White House, October 14, 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/; *see* "Update on the International Counter-Ransomware Initiative," U.S. Department of State, October 15, 2021, https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative.

[88] Comment by Interactive Advertising Bureau Poland.

[89] Comments by American Chamber of Commerce in Poland, Comments by Gloria Gonzalez Fuster and Laura Drechsler, Confederation of Finnish Industries EK, Interactive Advertising Bureau Poland (IAB Poland), Comments of Jussi Makinen, Ministry of Justice and Security, Comments of Peter Swire & DeBrae Kennedy-Mayo, techUK, U.S. Chamber of Commerce, US Mission to the EU.

Some countries may wish to have obstacles to information sharing, especially related to surveillance by the intelligence agencies of foreign countries, such as from China, Russia, or the U.S. National Security Agency.[90] Data localization can be seen as a way to increase the cost of surveillance of foreign citizens and "reduce comparative advantage of economies of surveillance."[91]

In response, we note that numerous types of information sharing discussed above have important benefits but little or no connection to collection of foreign intelligence. A general ban on data transfer, due to concern about surveillance, thus could be very over-broad. Second, a variety of multi-lateral efforts are underway to develop principles for government access to data held by private actors, including in the Organization for Economic Cooperation and Development[92] and the Global Privacy Assembly.[93] These efforts are focused directly on reducing the risk from surveillance, especially from other democratic countries. Third, the

---

[90] "Data localization provides better information security against foreign intelligence agencies." John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both," International Journal of Law and Information Technology, Volume 25, Issue 3, Autumn 207, pp. 213-232, at https://academic.oup.com/ijlit/article/25/3/213/3960261.

[91] Given the extent of the NSA's capabilities, it is unlikely that implementing data localization in a country would provide complete protection to the citizens of that country. However, even if complete protection was not possible, it is possible that data localization would increase the cost of surveillance of foreign citizens for the NSA (and other foreign intelligence agencies) and reduce the comparative advantage that it currently enjoys in the economies of surveillance as compared to the signals intelligence agencies in other jurisdictions. While this would not have much impact on NSA surveillance of high-value political or business leaders, it could make it more expensive for the NSA to conduct as wide-spread mass surveillance on the citizens of other countries as it currently does. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both," International Journal of Law and Information Technology, Volume 25, Issue 3, Autumn 207, pp. 213-232, at https://academic.oup.com/ijlit/article/25/3/213/3960261; *see generally* Ross Anderson, "Post-Snowden: The Economies of Surveillance," Light Blue Touchpaper, May 27, 2014, at https://www.lightbluetouchpaper.org/2014/05/27/post-snowden-the-economics-of-surveillance/ (discussion of concept of "economies of surveillance").

[92] "Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy," Organization for Economic Cooperation and Development (OECD), December 2020, at https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm; *see* Robert Williams, "Reckoning with Cyberpolicy Contradictions in Great Power Politics," Brookings TechStream, October 12, 2021, at https://www.brookings.edu/techstream/reckoning-with-cyberpolicy-contradictions-in-great-power-politics/.

[93] Adopted Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes, 43rd Closed Session of the Global Privacy Assembly, October 2021, https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf.

discussion above provided details from previous research efforts about when data sharing indeed is justified. In short, a blanket ban on data sharing across borders would appear over-broad.

V. Conclusion

Hard data localization, which blocks categories of transfers, has numerous effects on the ability of organizations to defend against cyberattacks. In some ways, expert commentators have already been aware of the problem, as shown by the numerous comments to the EDPB Guidance that mention possible effects on cybersecurity. Our research has drawn on these comments as a rich source of examples of possible problems. In addition, our step-by-step analysis of ISO 27002 has used that widely-recognized standard to show how pervasive the effects would be.

Based on this research, we have put forward a new organizing framework for understanding the effects of data localization. First, within an organization, data localization creates many obstacles to integrated management of cybersecurity risk – 13 of the 14 ISO 27002 controls, as well as additional sub-controls. Second, where an organization pays for third-party cybersecurity services, data localization creates numerous and severe obstacles to protecting cybersecurity, for that very large and growing market for services. Perhaps most generally, localization will cut a country off from the state-of-the-art in protecting against cybersecurity risk. Third, where an organization does not pay third parties, the important category of "information sharing" would be greatly affected by limits on transferring such information.

This study on the risks of data localization for cybersecurity leaves for future research important, related topics. For instance, this paper does not analyze the likely risks and benefits from data transfers for numerous specific scenarios, for cybersecurity and more generally. In addition, the paper does not examine the effects of localization in facilitating or hindering offensive cybersecurity actions, nor more general effects localization may have on each nation's definition of national security.

With that said, this paper explains numerous, significant reasons why hard data localization creates risks to cybersecurity. Until and unless proponents of localization address these concerns, scholars, policymakers, and practitioners have strong reason to consider significant cybersecurity harms in any overall analysis of whether to require localization.

[Appendix A begins on next page]

Appendix A: ISO 27002 Controls and Data Localization

This Appendix examines potential and apparent data localization effects, for a regime that blocks transfer of personal data (personally identifiable information). The Appendix lists each relevant portion of ISO 27002.[94] It discusses ways that localization requirements would appear to create risks to integrated cybersecurity management for an organization that operates both inside and outside of the jurisdiction that requires localization.

27002 Standard	Possible risks from localization
1. Scope 2. Normative references 3. Terms and definitions 4. Structure of this standard	27002 parts 1 to 4 do not contain specific security controls.
5. Policies for information security	Policies, instead of being global, must specify what actions are permitted in each country or region that requires localization.
6. Organization 6.1 Internal organization	Specification of roles may require escalation of roles, to enable control within each country or region that requires localization. Such escalation of privileges creates risk compared to the policy of least privilege. For Instance, "Care should be taken that no single person can access, modify, or use assets without authorization or detection." Such limits on the access of an individual becomes more difficult with more segregation within a company system.
6.2 Mobile devices and work	If a mobile device, such as a phone or laptop, is carried from one jurisdiction to another, then management of the mobile device may not be permissible remotely from the initial jurisdiction. For instance, a U.S. company may not be able to manage a Mobile Device Management program when an employee goes to the EU.

[94] For the text of ISO 27002, see https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf.

	For telework, there may be limits on the ability of an out-of-jurisdiction manager to oversee security for an employee within the jurisdiction.
7. Human resource security	There may be limits on the ability of an out-of-jurisdiction manager to oversee actions of an in-jurisdiction employee. For example, it may not be lawful for the out-of-jurisdiction manager to know which local employees have completed mandatory training.
8. Asset management 8.1 Inventory management	"An organization should identify assets relevant in the lifecycle of information and document their importance." "For each of the identified assets, ownership of the asset should be assigned." Linking an asset to the responsible individual would appear to be personal data, so central management may not be able to receive that information.
8.2 Information Classification	"Owners of information assets should be accountable for their classification." The task of information classification, including legal compliance, should be assigned to individuals. Tracking that compliance would be tracking of personal data.
8.2.3 Handling of assets	"Maintenance of a formal record of the authorized recipients of assets." Tracking of those records is tracking of personal data.
9. Access control 9.2 User access management	Similar to inventory control, access control cannot be centrally managed if personal data about individual access is prohibited to the system owner. As a mitigation, in some instances an authentication function can be done locally, without having to go to the system manager.
9.2.5 Review of user access rights	"Asset owners should review users' access rights at regular intervals." With localization, it may not be permissible for an asset owner to be in a different jurisdiction than the user.

	As a more general point, it is not clear how auditing can occur over the entire system, if asset ownership and access rights have to be done separately within a jurisdiction.
10.Cryptography	In order to prove personal data is not being transferred, it may be unlawful for an organization to use end-to-end encryption. This sort of prohibition exists already in some regulated sectors, such as financial institutions that have to document communications between a broker and a client.
11. Physical and environmental security	These security measures are generally local. The exception is where back-ups are remote, and localization can block back-ups to other jurisdictions.
12 Operations security 12.1.1 Documented operating procedures 12.1.2 Change management 12.1.3 Capacity management 12.1.4 Separation of development, testing, and operational developments	Operating procedures and change management are examples of where localization may make it more difficult for management to ensure that all policies are being complied with. One specific challenge can be escalation – some issues or problems can be solved at the local/national level; others may only be resolved by specialized experts who may be outside of the jurisdiction. For capacity management, to the extent that it is unlawful to shift capacity to other countries, then that would be a risk to availability. It would generally be uneconomic to do development and testing in each country, for a globalized company; therefore, development and testing would usually be done centrally or in a subset of countries. Where testing data includes personal data (as it often would to determine how employees or users interact with the system), then limits on transfer may exclude testing data from countries that have localization rules. The operations may then be less

	secure in such countries, because testing would not be tuned to local conditions.
12.2 Protection from malware	Controls against malware, such as detecting use of unauthorized software, may not be centrally managed if such detection would include access across borders to personal data.
12.3 Backup	Some approaches to backup, such as sharding, routinely may transfer personal data in the course of ordinary operations. Such approaches may not be lawful where localization requirements exist. For backup of one data center or other site, localization would require any such backup to be only within that country rather than to backup facilities elsewhere. Nation-by-nation backup may be more costly generally. It would also prohibit backing up to a remote site outside of the country, such as to address the risk of earthquakes, hurricanes, or other disruptions specific to one country.
12.4 Logging and Monitoring: "Event logs recording user activities ... should be produced, kept, and regularly reviewed" Because event logs can contain personally identifiable information, "appropriate privacy protection measures should be taken." "Where possible, system administrators should not have permission to erase or de-activate logs of their own activities"	For privacy purposes, logging data may be retained for a shorter period. For reasons such as to assist in machine learning pattern recognition and for forensic investigations, a longer retention period may help protect cybersecurity. That tension between privacy and cybersecurity exists even in the absence of data localization. Localization may pose additional obstacles. For instance, forensic investigations may be blocked without access to IP addresses or other data held in the localizing jurisdiction. For machine learning and other methods for spotting risky IP addresses and other data, localization may prohibit sharing data across borders. To protect against the security risks posed by system administrators and others with privileged access, 12.4.3 suggests an intrusion detection system managed outside

	of the control of the system and network administrators. Such independent controls may be more difficult to establish and maintain if localization requires separate sub-systems in an organization's systems.
12.6 Technical vulnerability management "A current and complete inventory of assets is a prerequisite for effective technical vulnerability management."	As mentioned for 8.1, inventory management, localization may block an organization from having a current and complete inventory of assets. Personal data may also exist for other aspects of managing technical vulnerabilities. For instance, personal data may exist in inventories of whose devices to update or in audit logs. Localization may block flows of such personal data.
12.7 Information systems audit considerations	Localization can pose risks to the auditing process. For instance, system auditing would typically log what is sent from Alice to Bob. With localization, the records of both what Alice sent and what Bob received, needed to check accurate receipt, may not be available to the system owner. This lack of visibility may be managed if only one side of the interaction has localization, by sending the audit information to the country that requires localization; however, if both countries require localization, then accurate auditing may be unlawful, because personal data flows out of both countries are blocked.
13 Communications security 13.1 Network controls "appropriate logging and monitoring should be applied" Management activities should be closely coordinated "to ensure that controls are consistently applied across the information processing infrastructure"	Localization may make it more difficult to conduct appropriate logging and monitoring, and to coordinate consistently across the organization's information processing infrastructure.

13.1.2 Security of network services	13.1.2 addresses the common situation where an organization relies on an outside vendor for network services. Localization in general will reduce the number and variety of providers that are available in the jurisdiction. Specifically, the locally available services may not have all of the cybersecurity features and quality that may be available from other countries. Examples of network services likely affected in this way would include cloud services, software as a service, platform as a service, and infrastructure as a service.
13.1.3 Segregation in networks	13.1.3 addresses a topic directly relevant to localization – segregation of networks. The text states: "The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination." The text does not contemplate segregation based on national borders. To the extent localization alters the optimal cybersecurity and cost decisions on how to segregate, the organization would undergo added costs and cybersecurity risk.
13.2 Information transfer 13.2.2 Agreements on information transfer "Agreements should address the secure transfer of business information between the organization and external parties." 13.2.3 Electronic messaging 13.2.4 Confidentiality or non-disclosure agreements	13.2 provides implementation guidance to protect the transfer of information. With localization, lack of such policies or violations of such policies may be unlawful, so organizations will have compliance obligations related to localization. The compliance obligations will exist as well for agreements with external parties. Additional confidentiality and non-disclosure agreements may be required to enforce localization. Governance of electronic messaging includes "legal considerations," such as localization prohibitions on transferring personal data

	through electronic messaging. Compliance regimes in emails may not readily exist to prevent such cross-border transfers.
14 System acquisition, development, and maintenance 14.1 Security requirements of information systems "Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks." 14.2 Security in development and support processes	As discussed previously, localization can create a variety of challenges for overall system management, such as by requiring segregation of systems to ensure that personal data cannot cross national borders.
14.3 Test data "Test data should be selected carefully, protected and controlled." "If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification." "System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data."	Although the use of operational data containing personally identifiable information "should be avoided," creating test data sets that are resistant to re-identification may be technically difficult or expensive. In light of broad legal definitions of what counts as "personal data" or PII, it may not be feasible to select test data that entirely lacks personal data. Creating sufficient test data, within each country, may be especially difficult for small- and medium-enterprises. To the extent that large companies may have greater access to sufficient test data by country than SME's, the cybersecurity of SME's may be disproportionately affected by localization.
15 Supplier relationships 15.1 Information security policy for supplier relationships	The contractual issues with suppliers are similar to the discussion of 13.1.2, Security of network services.
16 Information security incident management	**Detection.** By segmenting an organization's system, it may become more difficult to detect an intrusion. Suspicious activities in

	more than one country, if they involve IP addresses or if systems are fully segmented, would no longer be available in an organization-wide way. **Forensics.** Responding to breaches or other security incidents often includes a forensic component – seeking to understand as much as possible about the attack. To the extent that localization prohibits sharing information to those conducting the forensic investigation, that investigation may become less effective. **Deterrence.** To the extent attackers learn ways to take advantage of an organization's system segmented by country, they would face lower risk of detection. To the extent forensics generally is less effective, deterrence would be reduced. **Response.** Responding to breaches or other incidents often requires reporting to multiple authorities, often in different countries. Localization may create a conflict of laws, with the organization required to report by one country but forbidden to report by another.
17 Information security aspects of business continuity management 17.1 Information security continuity	To respond to adverse situations, such as a crisis or disaster, the organization should use "personnel with the necessary authority, experience and competence." If only in-country personnel can access the system, which contains personal data, such personnel may not be available during the crisis or disaster.
17.2 Redundancies "Information processing facilities should be implemented with redundancy sufficient to meet availability requirements."	Localization can reduce the ability of an organization to provide redundancy, to ensure confidentiality, integrity, and availability. For example, if there is one data center in a country, then localization could block back-ups and continuity plans that rely

"The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems."	on personal data that is stored in another country. On the other hand, if the redundancy exists in a different country, such as a backup data center, then there may be integrity or confidentiality risks arising from operations in that country. Technical measures may reduce such risks, however, such as if the cryptographic keys are held outside of the country that is not fully trusted.
18 Compliance 18 Compliance with legal and contractual requirements 18.1.4 Privacy and protection of personally identifiable information Depending on national legislation "controls may impose duties on those collecting, processing and disseminating personally identifiable information, and may also restrict the ability to transfer personally identifiable information to other countries."	In general, each localization rule obligates the organization to add compliance to its pre-localized baseline. 18.1.4 explicitly recognizes an organization's duties to comply with national legislation, which may "restrict the ability to transfer personally identifiable information to other countries."
18.2 Information security reviews 18.2.1 Independent review of information security "Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security."	Localization may, depending on how it is implemented, make it difficult or impossible for a unified independent review to take place on the entire system of the organization. The reason is that personal data in one country may not be reviewable from another country, limiting the scope of the independent review.