Arizona Law Journal of Emerging Technologies

*Volume 8* *Article 3*

3-2025

# THE RISKS TO CYBERSECURITY FROM DATA LOCALIZATION — ORGANIZATIONAL EFFECTS

Peter Swire & DeBrae Kennedy-Mayo
*Georgia Institute of Technology*

2024-2025 https://azlawjet.com Vol. 8, Art. 3

Arizona Law Journal of Emerging Technologies

# The Risks to Cybersecurity from Data Localization — Organizational Effects

*Peter Swire, J.Z. Liang Chair in the School of Cybersecurity and Privacy at the Georgia Tech College of Commuting, Professor of Law and Ethics at the Georgia Institute of Technology, Research Director of the Cross-Border Data Forum, and senior counsel with the law firm of Alston & Bird.*

*DeBrae Kennedy-Mayo, Faculty of Law & Ethics in the Scheller College of Business at the Georgia Institute of Technology, and senior fellow with the Cross-Border Data Forum.*

# Table of Contents

# THE RISKS TO CYBERSECURITY FROM DATA LOCALIZATION — ORGANIZATIONAL EFFECTS

Peter Swire & DeBrae Kennedy-Mayo[1]

## I. Abstract

This paper provides the first systematic analysis of the types of risks that data localization creates for cybersecurity management. Rather than protecting cybersecurity, data localization often creates obstacles to integrated management of cybersecurity risks, reduces the effectiveness of purchasing cybersecurity-related services, and systematically disrupts information sharing.

Part II introduces key concepts. The importance of data localization has risen rapidly in recent years, including in China, the EU, and India. This paper focuses on the effects of *"hard" data localization*, where transfer of data is prohibited to other countries. 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.

Part III examines privacy and non-privacy reasons driving localization laws. This discussion concludes that in general the rationale for localization does not alter the analysis of cybersecurity risks.

Part IV addresses the research methodology. In addition to a traditional literature review, we review approximately 200 comments recently submitted to European regulators concerning data transfers. Next, we analyze International Standards Organization ("ISO") 27002, to systematically examine the effects that localization rules for personal data would have on that widely-used set of cybersecurity management controls.

Part V 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*. By examining each control (and important sub-controls), we show that 13 of the 14 ISO 27002 controls would be

[1] Peter Swire is the J.Z. Liang Chair in the School of Cybersecurity and Privacy, in the Georgia Tech College of Commuting, and Professor of Law and Ethics at the Georgia Institute of Technology. He is the Research Director of the Cross-Border Data Forum and senior counsel with the law firm of Alston & Bird. DeBrae Kennedy-Mayo is Faculty of Law & Ethics 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 other person. An earlier version of this article was first posted to SSRN on February 18, 2022.

negatively affected by localization of personal data. Second, data localization pervasively limits *provision of cybersecurity-related services by third parties*, a global market of roughly $300 billion annually. Notably, a region requiring localization would cut its organizations off from best-in-class cybersecurity services, thereby making its organizations easier targets for attackers. Third, localization undermines *information sharing for cybersecurity purposes*. For each of these effects of data localization on cybersecurity, we will briefly examine the primary counter arguments to our position. Part VI is the conclusion.

## II. Introduction

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.[2] This paper examines a prominent category of such laws — data localization laws, focusing on the requirements for localization of personal data.

The importance of data localization has risen rapidly in recent years, including for the three major geographies 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.[3] Second, the EU has taken significant steps towards localization of personal data in the wake of the 2020 *Schrems II* decision of the European Court of Justice.[4] Among enforcement actions after the *Schrems II* decision, the Portuguese data protection authority ordered a government agency to terminate its use of cybersecurity services from U.S.-based Cloudflare.[5] Despite the finalization of the EU-U.S. Data Privacy Framework in July 2023, legal challenges in the EU are expected regarding this most recent agreement, which could jeopardize these transatlantic data flows.[6] In the

---

[2] Bruce Schneier, *Technologists vs. Policy Makers*, SCHNEIER ON SEC. (Jan./Feb. 2020), https://www.schneier.com/essays/archives/2020/02/technologists_vs_pol.html.

[3] Jinhe Liu, *China's Data Localization,* 13 CHINESE J. COMMC'N 84, 87 (2020); *see* Hunter Dorwart, *New FPF Report: Demystifying Data Localization in China – A Practical Guide,* FUTURE OF PRIV. F. (Feb. 21, 2022), https://fpf.org/blog/new-fpf-report-demystifying-data-localization-in-china-a-practical-guide/.

[4] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems, Judgment of the Court (Grand Chamber), (European Court of Justice, July 16, 2020).

[5] Peter Swire & DeBrae Kennedy-Mayo, *New Urgency About Data Localization with Portuguese Decision,* IAPP: PRIV. PERSPECTIVES (Apr. 29, 2021), https://iapp.org/news/a/new-urgency-about-data-localization-with-portuguese-decision/#.

[6] Laura Kayali, *French Lawmaker Challenges Transatlantic Data Deal Before EU Court,* POLITICO (Sept. 7, 2023, 7:00 PM), https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-before-eu-court/; Foo Yun Chee, *EU Seals New U.S. Data Transfer Pact, But Challenge Likely,* REUTERS (July 10, 2023, 12:00 PM), https://www.reuters.com/technology/eu-announces-new-us-data-transfer-pact-challenge-ahead-2023-07-10/; *see* Data Transfers, *European Commission Gives EU-U.S. Data Transfers Third Round at CJEU*, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu; *see* Emily Benson & Elizabeth Duncan, *Temporarily Shielded? Executive Action and the Transatlantic Data Privacy Framework,* CSIS (Oct. 7, 2022), https://www.csis.org/analysis/temporarily-shielded-executive-action-and-transatlantic-data-privacy-framework; *see also* Théodore Christakis et al., *The Redress Mechanism in the Privacy Shield Successor: On the Independence*

Data Act and other proposed legislation, the EU would also impose localization rules for non-personal data, such as "connected machines or connected devices."[7] Third, India has required data localization for financial transactions.[8] India's legislature seriously considered extending the proposed Data Protection Bill to cover communications and other personal data more broadly.[9] As Nigel Cory and Luke Dascoli have documented, the number of data localization measures roughly doubled from 2017 to 2021, including at least 62 countries with 144 restrictions.[10]

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 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.[11]

The focus is 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.[12] The paper does not seek to analyze other aspects of security, including offensive cyber measures and government surveillance used to protect national security. The paper also makes the reasonable assumption that measures that impair cybersecurity defenses have a negative effect on overall cybersecurity. We provide details about such impairment in a companion paper, on "Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and

*and Effective Powers of the DPRC,* IAPP (Oct. 11, 2022), https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/.

[7] *Data Act*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/data-act (last updated Apr. 4, 2024); *see* Kenneth Propp, *Cultivating Europe's Digital Garden,* LAWFARE (March 4, 2022, 9:01 AM), https://www.lawfaremedia.org/article/cultivating-europes-data-garden.

[8] Peter Swire et al., *India's Access to Criminal Evidence in the US: A Proposed Framework for an Executive Agreement,* OBSERVER RSCH. FOUND. (Apr. 10, 2023), https://www.orfonline.org/research/indias-access-to-criminal-evidence-in-the-us/.

[9] Anirudh Burman, *Understanding India's New Data Protection Law,* CARNEGIE INDIA (Oct. 3, 2023), https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624; Nitin Dhavate & Ramakant Mohapatra, *A Look at Proposed Changes to India's (Personal) Data Protection Bill,* IAPP: PRIV. TRACKER (Jan. 5, 2022), https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/; Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,* INFO. TECH. & INNOVATION FOUND. (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

[10] Cory & Dascoli, *supra* note 9.

[11] *See* Nigel Cory, *How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime*, INFO. TECH. & INNOVATION FOUND. (July 8, 2021), https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data.

[12] NAT'L INST. OF STANDARDS & TECH., THE NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 3–4 (2024) (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.").

Procedures."[13] That paper draws on the MITRE ATT&CK Framework and other frameworks for assessing types of attacks.[14] That research highlights how localization, for instance, undermines the defender's ability to discern the "who and what" of attacks, such as efforts by an attacker to escalate privileges. Localization also creates risks when the defenders know less than the attackers, such as limits on penetration testing that accesses data across continents. Another companion paper has recently addressed "Legal Issues in Reconciling Data Protection, AI, and Cybersecurity under EU Law," highlighting certain risks under EU law, from data localization, especially for updating threat analysis for cybersecurity services and for training artificial intelligence models.[15]

This paper explores the effects of localization in general, rather than for specific technologies. Some localization measures arise from privacy laws and target personal data. For example, such measures could limit transfer of IP addresses linkable to individuals, which are considered "personal data" in the EU under the EU General Data Protection Regulation ("GDPR") and are widely used in cybersecurity.[16] Other proposed localization measures, by contrast, would target non-personal data, applying to machine-to-machine data used for cybersecurity purposes. In addition to whether a measure addresses personal or non-personal data, localization measures might vary, for instance, in terms of which exceptions, if any, allow transfers to continue. As these examples of localization measures for personal data and non-personal data illustrate, the scope of each localization measure, and consequent effects on specific cybersecurity technologies, will thus vary depending on the terms of that localization measure.

Part III presents research for this paper. Our literature review found no previous systematic discussion of these issues. To explore the effects of data localization, much of the discussion will focus on the de facto data localization of personal data in the EU as well as the potential for significant data localization mandates in India. A main reason for the focus on the EU and India is the significance of the impacts on global data flows resulting from the actions of the respective governments. Another reason for the focus on the EU and personal data 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, and that guidance was finalized in mostly similar form in 2021.[17] Professor Théodore Christakis explained that this "EDPB Guidance seems

---

[13] *See generally* Peter Swire et al., *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures,* 9 J. OF CYBER POL'Y 20, 20–51 (2024).

[14] *ATT&CK,* MITRE, https://attack.mitre.org/ (last visited Nov. 7, 2023); *see What Is the MITRE ATT&CK Framework?*, CROWDSTRIKE (Sep. 20, 2023), https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/.

[15] *See generally* Iain Nash et al., *Legal Issues in Reconciling Data Protection, AI, and Cybersecurity Under EU Law*, 89 MO. L. REV. 871, 871–939 (2024).

[16] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, Judgment of the Court (Second Chamber), (European Court of Justice, Oct. 19, 2016).

[17] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUR. DATA PROT. BD. (Dec. 19, 2020), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en ; *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUR. DATA PROT. BD. (June 18, 2021), https://edpb.europa.eu/

nonetheless to prohibit almost all such transfers when the personal data is readable [i.e. non-encrypted] in the third country."[18] 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 of personal data.[19]

The examples of the EU and India help illustrate how the effects of localization vary based on the number of jurisdictions with localization rules and the location of an organization's cybersecurity management. As a simplified example, first suppose that an organization does business in the EU and the U.S., but with cybersecurity management in the U.S. If the EU has hard data localization, then that law would prohibit U.S. management from viewing account information and other data processed in the EU. Second, for an organization doing business in both jurisdictions, suppose that the organization decided to centralize all cybersecurity management in the EU. This approach would keep all of the regulated data in the EU, with management in the EU. We call this the *"black hole effect,"* in the sense that data gets pulled into one place (the EU) but cannot go back out from the EU. Such an approach might in theory help "solve" some of the cybersecurity problems from localization, but only if it is technically feasible and economical to manage cybersecurity without regulated data going to other jurisdictions. Third, suppose that more than one jurisdiction requires localization, such as the EU and India. In this scenario, the organization can no longer centralize system management in one jurisdiction: data from the EU cannot go to India, and data from India cannot go to the EU. *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 forensics concerning data breaches.*

Part V provides a new categorization of the effects of data localization on cybersecurity management. To date, there has been no proposed method for categorizing and identifying the effects of localization measures. To systematize the range of possible effects, we categorize by the organizational form — effects within the organization, across organizations with payment, and across organizations without payment. First, our analysis shows that data localization would threaten an organization's ability to achieve *integrated management of cybersecurity risk*. We analyze International Standards Organization ("ISO") 27002, as a way to systematically examine the effect of data

---

our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[18] Theodore Christakis, "*Schrems III?" First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 3),* EUR. L. BLOG (Nov. 17, 2020), https://www.europeanlawblog.eu/pub/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/release/1.

[19] 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 F. (Apr. 29, 2021), 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/.

localization on that widely-used set of cybersecurity management controls.[20] Our analysis shows how 13 of the 14 relevant ISO 27002 controls, as well as multiple sub-controls, would be affected by localization of personal data. Second, the analysis explains how data localization pervasively limits *provision of cybersecurity-related services by third parties*, a global market of roughly $300 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 briefly examine the primary counter arguments to our position. Part VI is the conclusion.

# III. 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 that are 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."[21]

## 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

[20] At the time of our initial research, ISO 27002 (2013) was in effect. INT'L ORG. FOR STANDARDIZATION, *ISO/IEC 27002:2013* (Nov. 1, 2013), https://www.iso.org/standard/54533.html. In February 2022, ISO published an updated version. ISO 27002 (2022). INT'L ORG. FOR STANDARDIZATION, *ISO/IEC 27002:2022* (Feb. 2022), https://www.iso.org/standard/75652.html.
[21] Cory & Dascoli, *supra* note 9.

information."[22] 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."[23] 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.[24] Second, beyond encryption, there has been substantial work done on "privacy enhancing technologies," ("PETs") including by the European Union Agency for Cybersecurity ("ENISA").[25] These PETs help with privacy because fewer recipients see 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.[26] Although providing one definition of "privacy" is notoriously 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.[27] 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*.[28] Suppose, as a hypothetical, that data localization (enacted on the premise that it protects privacy) prevents cyber-attack detection or reduces the ability to identify the

[22] Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1522 (2002); *see also* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 670 (2013).
[23] Swire & Steinfeld, *supra* note 22.
[24] Giovanni Buttarelli, *Cybersecurity Under the Next President: A Symposium with Cybersecurity Industry Leaders. Closing Speech at Coalition for Cybersecurity and Law Symposium,* EDPS (Nov. 15, 2016), https://edps.europa.eu/sites/default/files/publication/16-11-15_speech_gb_cybersecurity_en.pdf.
[25] ENISA, DATA PROTECTION ENGINEERING: FROM THEORY TO PRACTICE 6–9 (2022); ENISA, READINESS ANALYSIS FOR THE ADOPTION AND EVOLUTION OF PRIVACY ENHANCING TECHNOLOGIES METHODOLOGY, PILOT ASSESSMENT, AND CONTINUITY PLAN 5–52 (2015).
[26] *See* John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INT'L J. L. & INFO. TECH. 213, 218–19 (2017); Anupam Chander & Uyên P. Lê, *Data Nationalism,* 64 EMORY L. J. 677, 718–21 (2015); McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law,* 44 GEO. WASH. INT'L. REV. 643, 681–91 (2012); Bruce Schneier, *Security vs. Privacy*, SCHNEIER ON SEC. (Jan. 29, 2008, 5:21 AM), https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html.
[27] PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY 74 (4th ed. 2024).
[28] *See* Swire et al., *supra* note 13; *see also* PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27, at 74–77.

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.[29] Cybersecurity traditionally concerns CIA — confidentiality, integrity, and availability.[30] 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.[31] 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.[32] If a privacy measure makes it more difficult to resist a DDOS attack, then stricter privacy protection is accompanied by an increased cybersecurity risk.[33] *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 the effects to improve privacy or reduce cybersecurity. Apart from the size of the 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 can also expand the attack surface, creating cybersecurity risks, potentially greater than the cybersecurity benefits.[34] 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.

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

[29] *See* MICHAEL NIELES ET AL., AN INTRODUCTION TO INFORMATION SECURITY 1–70 (Revision 1, 2017); *see also* PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27.
[30] *See* NIELES ET AL. *supra* note 29, at 2–3, 7; *see also* PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27.
[31] *See* Cameron Hashemi-Pour et al., *Digital Signature*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/digital-signature (last visited Jan. 8, 2025); PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27, at 73.
[32] *See* Swire, *supra* note 13; PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27, at 75–77.
[33] *See* Swire, *supra* note 13; PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 27, at 74–77.
[34] Colin Tankard, *3-2-1, No Thank You*, INFOSECURITY MAG. (Dec. 28, 2020), https://www.infosecurity-magazine.com/opinions/321-no-thank-you; *see also What Is an Attack Surface and 7 Ways to Minimize It*, BLUEVOYANT, https://www.bluevoyant.com/knowledge-center/what-is-an-attack-surface-and-7-ways-to-minimize-it (last visited Jan, 8, 2025).

as 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, conclude that GDPR's "significant cyber risks have been downplayed, if not ignored outright."[35] The official EU discussions to date have largely accentuated the positive aspects of the relationship between protecting privacy and cybersecurity.[36] Our research has uncovered almost no discussion of the tension between cybersecurity and privacy 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 example, the Article 29 Data Protection Working Party's 2014 discussion of the lawful processing of data notes that "IT and network security" qualifies as one of "the most common contexts" where legitimate interests can be balanced against the interests and rights of data subjects – thus identifying cybersecurity as an area that falls into the balancing test laid out in the present-day Article 7 of the GDPR.[37] The Working Party, however, concluded its discussion by stating that "an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws."[38] The European Data Protection Board (EDPB) incorporated this interpretation in its 2019 guidelines on processing personal data for online services.[39] In 2021, the European Data Protection Supervisor (EDPS) issued an opinion on the EU's cybersecurity strategy and updates to the Network and Information Security Directive.[40] 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."[41] It then recognized that pursuing cybersecurity may lead to "deploying measures that interfere with the rights to data protection and privacy of individuals."[42] The EDPS stated that any potential limitation on those rights must meet the strict requirements of

[35] ROSLYN LAYTON & SILVIA ELALUF-CALDERWOOD, A SOCIAL ECONOMIC ANALYSIS OF THE IMPACT OF GDPR ON SECURITY AND PRIVACY PRACTICES 4 (12th CMI Conference on Cybersecurity and Privacy (CMI), 2019).
[36] *See* Selby, *supra* note 26, at 230–31.
[37] ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 06/2014 ON THE NOTION OF LEGITIMATE INTERESTS OF THE DATA CONTROLLER UNDER ARTICLE 7 OF DIRECTIVE 95/46/EC 24–25 (2014).
[38] *Id.* at 25.
[39] *See generally* EUR. DATA PROT. BD., GUIDELINES 2/2019 ON THE PROCESSING OF PERSONAL DATA UNDER ARTICLE 6(1)(B) GDPR IN THE CONTEXT OF THE PROVISION OF ONLINE SERVICES TO DATA SUBJECTS (2019).
[40] *See generally* EUR. DATA PROT. SUPERVISOR, OPINION 5/2021 ON THE CYBERSECURITY STRATEGY AND THE NIS 2.0 DIRECTIVE (2021); THE EUR. PARLIAMENT & THE COUNCIL OF THE EUR. UNION, DIRECTIVE (EU) 2016/1148 (2016); Dimitra Markopoulou et al., *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35 COMPUT. L. & SEC. REV. 1 (2019).
[41] EUR. DATA PROT. SUPERVISOR, *supra* note 40, at 7.
[42] *Id.* at 7–8.

Article 52(1) of the EU Charter of Fundamental Rights.[43] That Article notably states that any limitations on rights must "respect the essence of those rights and freedoms."[44] 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."[45] The 2023 implementation of the EU's Network and Information Security (NIS 2) Directive — an EU-wide cybersecurity mandate — appears to continue this trend.[46] The Directive, which places affirmative duties on covered entities to share information about cybersecurity incidents within certain time frames, acknowledges that cybersecurity involves "the management of vulnerabilities, cybersecurity-risk management measures, reporting requirements, and cybersecurity information-sharing arrangements."[47] To further these activities, the Directive instructs that "Member States can cooperate with third countries and undertake activities . . . including information exchange on cyber threats, incidents, vulnerabilities, tools and methods, tactics, techniques, and procedures, cybersecurity crisis management preparedness, and exercises, training, trust building and structured information-sharing arrangements."[48] The Directive permits computer security incident response teams (CSIRTs) to "exchange relevant information with third countries' national security incident response teams, including personal data . . . ."[49] The Directive also allows the EU to engage in international cooperation related to cybersecurity.[50] Both provisions for interacting with third countries conclude with the requirement that the data sharing must comply with EU data protection law.[51] 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).[52]

## B. Data Localization for Non-Privacy Reasons

For the EU, legal developments in data protection law, including the *Schrems II* decision and the EDPB Guidance, drive the de facto shift toward data localization.[53] A range of rationales, in addition to privacy protection, can support data localization. In their review of recent localization measures, Cory and Dascoli wrote:

[43] *Id.*
[44] EUR. UNION AGENCY FOR FUNDAMENTAL RTS., EU CHARTER OF FUNDAMENTAL RIGHTS ARTICLE 52(1) (2009).
[45] *Id.*
[46] *See generally* Council Directive 2022/2055, 2022 O.J. (L 333).
[47] *Id.* at 74.
[48] *Id.*
[49] *Id.* at art. 10; *see Id.* at 45, 74.
[50] *Id.* at art. 17; *see Id.* at 73–74.
[51] *Id.* at art. 10; *Id.* at art. 17.
[52] One recent article critiques EU enforcers' focus on transfers to third countries rather than addressing greater cybersecurity risks, such as data breaches, noting that "[t]he emphasis on transfers should not be at the expense of security more generally." W. Kuan Hon, *Transfers Takeaways from GDPR Enforcement in Cloud Computing & Beyond,* SSRN, Jan. 28, 2022, at 1, 13.
[53] Cory, *supra* note 11.

> 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.[54]

Cory and Dascoli discuss a range of objectives for data localization, including data sovereignty, censorship, and implementation of law enforcement and regulatory oversight.[55] 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 discuss the effects of data localization on cybersecurity, which, unless noted, do not depend on the rationales for localization.

## IV. 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.[56] A variety of publications have discussed how data localization may affect cybersecurity, often as a paragraph or a few sentences in a broader discussion of data localization.[57] 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.[58] 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."[59] When

[54] Cory & Dascoli, *supra* note 9.
[55] *Id.*
[56] *See* Yantsislav Yanakiev & Todor Tagarev, *Governance Model of a Cybersecurity Network: Best Practices in the Academic Literature*, COMPSYSTECH '20 27, 27–34 (2020); *see* Pierantonia Sterlini et al., *Governance Challenges for European Cybersecurity Policies: Stakeholder Views*, CYBER SEC. FOR EUR. (May 2019), https://cybersec4europe.eu/wp-content/uploads/2019/11/Governance-Challenges-for-European-CyberSecurity-Policy_-Stakeholders-Views_V.Def_.pdf; *see* Josep Domingo-Ferrer et al., *Canvas White Paper 4 - Technological Challenges in Cybersecurity,* CANVAS, Dec. 28, 2017, at 1; *see* Richard D. Taylor*, "Data Localization": The Internet in the Balance,* 44 TELECOMMS. POL'Y 102003 (2020); *see* David Lore, *Reconciling Data Localization Laws and the Global Flow of Information*, CYBERSECURITY L. REP. (Oct. 11, 2017), https://www.cslawreport.com/2564131/reconciling-data-localization-laws-and-the-global-flow-of-information.thtml; *see* W. Kaun Hon et al., *Policy, Legal, and Regulatory Implications of a Europe-Only Cloud*, 24 INT'L J. L. & INFO. TECH. 251 (2016).
[57] *See generally* Yanakiev & Tagarev, *supra* note 56; Sterlini et al., *supra* note 56; Domingo-Ferrer et al., *supra* note 56; Taylor*, supra* note 56; Lore, *supra* note 56; Hon et al., *supra* note 56.
[58] Susan Lund & James Manyika, *Defending Digital Globalization.* MCKINSEY GLOB. INST. (Apr. 20, 2017), https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization.
[59] *Id.*

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.[60] The OECD, in its 2020 report on data localization trends and challenges, pointed out that the relationship that includes data localization and cybersecurity is "a subject ripe for further research."[61] In addition, to provide additional insights, we have presented our research at conferences, including RSA and the Cybersecurity Law and Policy Scholars Conference, and interviewed several cybersecurity experts, including senior security engineers in major companies, government officials, and lawyers who specialize in data breaches and international data transfers.

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, with our research details posted publicly,[62] approximately 25% of the nearly 200 comments submitted to the EDPB expressed concern that the Draft Guidance would result, in practice, in data localization.[63] 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," transform the EU into a "digital island," and "balkanize global data flows."[64]

Although the comments do not reflect a random sample of experts' views, the comments provide useful information and accompanying explanation from a wide variety of expert commenters, from many different countries.

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 on key cybersecurity management controls, specifically concerning personal data. The best-known ISO cybersecurity standard is ISO/IEC 27001 ("ISO 27001"). ISO 27001 sets forth specifications for an information security management system, providing an overall risk-based framework for managing an organization's

[60] Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 783 (2020).
[61] Dan Svantesson, *Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines*, OECD DIGITAL ECON. PAPERS, Dec. 22, 2020, at 1, 14–15.
[62] The detailed results are available for view at PeterSwire.net. Peter Swire & DeBrae Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity*, PETER SWIRE, https://peterswire.net/wp-content/uploads/Detailed-Research-on-Comments-Data-Localization-and-Cybersecurity-05042022.pdf (last visited Nov. 7, 2023).
[63] *Id.*; *see also Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17.
[64] Kennedy-Mayo & Swire, *supra* note 19 (Comment by Employers of Poland (Poland), Comment 11; Comment by U.S. Chamber of Commerce (U.S.), Comment 63; Comment by Polish Confederation Lewiatan (Poland), Comment 105; Comment by City of London Law Society (U.K.), Comment 155.).

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 controls."[65] Below, we examine each ISO 27002 control, and relevant sub-controls, and consider the potential effects of localizing personal data.

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, discussed further below, that were not identified in the literature review and EDPB comments. Such examples, which have been discussed little to date, include auditing, logging, and comprehensive monitoring of the workings of an organization's systems.[66] 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.

# V. Categorizing the Effects of Data Localization on Cybersecurity

We now categorize effects of data localization based on the organizational form — effects within the organization, across organizations with payment, and across organizations without payment. 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.

## 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

[65] ISO/IEC 27002:2013, *supra* note 20.
[66] *See infra* notes 79–80, 83–91.; *see also* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS 94–97 (Brookings Institution Press, 1998).

paper does not seek to make legal conclusions about which national laws prohibit which categories of data flows.[67]

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 in the U.S. in situations where those experts would have access to the data.[68] However, countries with localization rules could make an exception which was crafted to encompass concepts of necessity and proportionality, 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.[69]

With that said, we discuss the EU and India as two important geographies that have recently increased limits on data transfers. 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, showing how 13 of the 14 relevant controls would be negatively affected. We next provide examples

[67] For example, the 2022 academic paper entitled "Processing of Botnet Tracking Data under the GDPR" provides detailed analysis of the differing legal bases for processing data related to botnet tracking for three scenarios: research in the public interest, commercial interest of security companies, and commercial interest of Internet service providers. Leon Bock et al., *Processing of Botnet Tracking Data under the GDPR,* 45 COMPUT. L. & SEC. REV., 105652, 1–2, 6–16 (2022).

[68] The experts might undergo the travel time and expense to visit the country having the problem, but would not be able to return home with localized information on their devices. Such a work-around to localization may sometimes be feasible, but with higher costs and the risk of lower efficacy.

[69] 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. *See, e.g.,* EUR. DATA PROT. SUPERVISOR, ASSESSING THE NECESSITY OF MEASURES THAT LIMIT THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA: A TOOLKIT (2017). Another possibility would be to follow the OECD approach of applying the proportionality test to the data localization measure. According to the OECD's 1980 Privacy Guidelines, "data privacy laws typically serve the dual purposes of: (1) ensuring the protection of personal data, and (2) facilitating privacy-respecting transborder data flows." Svantesson, *supra* note 61, at 24. These guidelines provide that "any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing." *Id.* at 27. In 2013, the OECD clarified that the proportionality assessment intends to ensure that any restrictions imposed by countries on cross-border data flows do "not exceed the requirements necessary for the protection of personal data." *Id.*

from the comments to the EDPB of ways that data localization creates obstacles to integrated management.

### *1. ISO 27002 Controls*

To assess the possible effects of localization on the ISO 27002 controls, we begin with the EU's broad definition of "personal data." Article 4 of GDPR defines "personal data" to include "any information relating to an identified or identifiable natural person."[70] EU law has developed the definition of "personal data" into an expansive concept that goes far beyond direct identifiers such as name or email. The definition also applies to any information "relating to" data that is "identifiable," and there is a large technical literature showing how difficult it is to effectively de-identify data.

Consider some of the ubiquitous ways that an organization's Chief Information Security Officer oversees activities that involve personal data. As a non-exhaustive list, here are some important categories:

I. Employee data, including name, username, and information "relating to" the activities of the employee.
II. Device and services data, including MAC addresses, other device IDs, and cookie IDs.
III. Actions taken by a user account (including customers and employees), including IP logs and detection of anomalous activity.
IV. Actions taken between accounts, such as traffic analysis that logs such activity or analyzes logs of such activity.

With this broad definition of personal data in mind, we examine each of the relevant ISO 27002 controls.[71] Due to space constraints, we provide relatively brief discussion of each control, but we believe we provide enough detail to indicate the range of effects from blocking transfer of personal data. Controls 1–4 are general topics, such as the scope of the standard, and do not contain specific security controls, so Controls 5–18 are the relevant controls.

**Control 5: Policies for Information Security**.[72] With localization, policies can no longer be optimized globally. Instead, policies would be changed to specify what actions are permitted in each country or region that requires globalization. Such complexity tends to increase risk for the cybersecurity defense.

[70] EUR. PARLIAMENT & COUNCIL OF THE EUR. UNION, GENERAL DATA PROTECTION REGULATION Article 4(1) (2016).
[71] ISO/IEC 27002:2013, *supra* note 20.
[72] *Id.* at 2–4.

**Control 6: Organization**.[73] The internal organization of cybersecurity would need to change with localization, so that the local administrator would have control within each jurisdiction that requires localization. Such escalation of privileges creates risk compared to the policy of least privilege. For instance, the standard says, "[c]are should be taken that no single person can access, modify, or use assets without authorization and detection."[74] Such limits on the access by an individual becomes more difficult with increased segregation within a company system.

**Control 7: Human resource security**.[75] Management of human resource data becomes far more complex with localization. An out-of-jurisdiction manager (outside of the country with localization) would face limits on ability to oversee an in-jurisdiction employee. As just one example, the manager would not be able to know which local employees (including the leader in-country) have completed mandatory cybersecurity or privacy training.

**Control 8: Asset management**.[76] Sub-controls here include inventory management, information classification, and handling of assets. The standard says, "[f]or each of the identified assets, ownership of the asset should be assigned . . . ."[77] Yet, an out-of-country manager would not be able to receive personal data about who is assigned to each asset. The standard also says, "[o]wners of information assets should be accountable for their classification."[78] The task of information classification, including legal compliance, should be assigned to individuals, who may work in a different country. Tracking that compliance would be tracking of personal data.

**Control 9: Access control**.[79] Similar to inventory management, access control cannot be centrally managed if personal data about individual access is prohibited to the system owner. The standard says, "[a]sset owners should review users' access rights at regular intervals[,]"[80] but an asset owner out-of-jurisdiction cannot review the access rights of an individual in-jurisdiction. As a more general point, it is not clear how auditing in general can occur over the entire system, if personal data about access ownership and access rights has to stay in-jurisdiction.

**Control 10: Cryptography**.[81] The analysis is somewhat distinct for this control. We note that encryption algorithms, and implementing cryptosystems, may not themselves require transfers of personal data. On the other hand, the organization for compliance purposes may need to prove that personal data has not been transferred illegally. This

[73] *Id.* at 4–8.
[74] *Id.* at 5.
[75] *Id.* at 9–13.
[76] *Id.* at 13–19.
[77] *Id.* at 13.
[78] *Id.* at 15.
[79] *Id.* at 19–28.
[80] *Id.* at 23.
[81] *Id.* at 28–30.

sort of prohibition already exists in regulated sectors, such as financial institutions, which must document communications between a broker and a client. Data localization rules thus are likely inconsistent with the use of end-to-end ("E2E") encryption — effective localization rules often will 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 a breach or concern about an illegal transfer.

**Control 11: Physical and environmental security**.[82] These security measures are generally local, and so this is the ISO 27002 control where we do not generally see effect from localization laws.

**Control 12: Operations Security**.[83] Localization would have multiple effects on Control 12, which defines multiple sub-controls.

> **Control 12.1: Operational procedures and responsibilities**.[84] This sub-control requires the system owner to document operating procedures and perform change management. Localization makes it far more difficult to monitor the entire system well enough to ensure that all policies are being complied with. The sub-control addresses capacity management — to the extent it is unlawful to shift capacity to other countries, that increases the risk to availability. The sub-control specifies separation of development, testing, and operational development. Such separation becomes more difficult or impossible, especially for small countries that mandate localization. Similar analysis applies for Control 12.5 (control of operational software).
>
> **Control 12.2: Protection from malware**.[85] Controls against malware, such as detecting use of unauthorized software, may not be centrally managed if such detection includes access across borders to account names, device IDs, or other personal data.
>
> **Control 12.3: Backup**.[86] Some approaches to backup, such as sharding, routinely transfer personal data in the course of ordinary operations. Such approaches would be unlawful where the sharding exists across borders. For backup of one data center or other site, localization would require any such backup to be only within the country rather than to backup facilities elsewhere. Nation-by-nation backup will likely be more costly generally. Localization would also prohibit backup to a remote site outside of the country, such as to address the risk of earthquakes or hurricanes, or the risk of military attacks such as Russia against Ukraine.

[82] *Id.* at 30–38.
[83] *Id.* at 38.
[84] *Id.* at 38–41.
[85] *Id.* at 41–42.
[86] *Id.* at 42–43.

**Control 12.4: Logging and Monitoring**.[87] This control states, "[e]vent logs recording user activities . . . should be produced, kept, and regularly reviewed."[88] It adds "[w]here possible, system administrators should not have permission to erase or deactivate logs of their own activities . . . ."[89]

The effects of localization on logging and monitoring apply differently depending on the location of where the organization does the logging and monitoring. As mentioned in the Introduction, the effects are substantial where cybersecurity is managed outside of the localizing jurisdiction, such as where management is in the U.S. for EU data, and management can no longer do monitoring of the organization's system from the U.S. Second, if two or more jurisdictions require localization, such as the EU and India, then there cannot be organization-wide logging and monitoring. Third, as we discussed for the "*black hole effect*," if only one jurisdiction requires localization, such as the EU, then the organization can seek to gather all of the regulated data into the EU, but many follow-up action items would entail transfer of personal data to the country where the follow-up is needed.

To protect against the security risks posed by system administrators and others with privileged access, this control also suggests having an intrusion detection system managed outside of the control of the system and network administrators. These sorts of independent controls would appear more difficult to establish and maintain if localization requires separate sub-systems in an organization's system, each based in the same country.

**Control 12.6: Technical vulnerability management**.[90] This control states, "[a] current and complete inventory of assets . . . is a prerequisite for effective technical vulnerability management."[91] This inventory includes personal data, such as user names and device IDs. Localization would limit transfers of this data used for the asset inventory. Similar problems apply to Control 12.7 (information systems audit considerations).

**Control 13: Communications security**.[92] The challenges from localization on communications security are similar to those for operations security. For communications, "appropriate logging and monitoring should be applied,"[93] and management activities should be closely coordinated "to ensure that controls are

[87] *Id.* at 43–45.
[88] *Id.* at 43.
[89] *Id.* at 44.
[90] *Id.* at 46–48.
[91] *Id.* at 46.
[92] *Id.* at 49.
[93] *Id.*

consistently applied across the information processing infrastructure . . . .”[94] Localization, however, poses obstacles to these activities.

> **Control 13.1.3: Segregation in networks**.[95] This sub-control addresses a topic directly relevant to localization — segregation in networks. The text states, “[t]he 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 . . . .”[96] 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 risks. In addition, segregation adds complexity to operating an organization, which often adds cybersecurity risk.
>
> **Control 13.2: Information transfer**.[97] This sub-control 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 contracts with external parties. Additional confidentiality and non-disclosure agreements may be required to enforce localization.
>
> Electronic messaging may pose particular compliance challenges. The organization would be legally required to ensure that personal data is not illegally transferred through emails and other electronic messaging. Compliance with localization thus may entail detailed surveillance of emails and other messaging, and compliance regimes to do so may not readily exist to prevent such cross-border transfers.

**Control 14: System acquisition, development, and maintenance**.[98] We highlight here two effects from localization.

> **Control 14.2: Security in development and support processes**.[99] Many organizations use a “follow the sun” approach for customer support, as well as for cybersecurity and other system support for employees. This approach often includes hiring personnel, in-house or by contract, who can cover time zones around the world. As a related support consideration, the organization often has layers of escalation for cybersecurity and other support. Routine matters may be handled by relatively junior people, in the home jurisdiction. When matters get

[94] *Id.*
[95] *Id.* at 50.
[96] *Id.*
[97] *Id.* at 50–54.
[98] *Id.* at 54.
[99] *Id.* at 57–62.

escalated and require special expertise, however, then the organization's best experts may not be in the home jurisdiction. In short, localization can raise support costs and mean that necessary expertise may no longer be available for the country that limits transfers of data to other countries.

**Control 14.3 Test data**.[100] State-of-the-art cybersecurity often relies on real-time and other automated approaches that rely on artificial intelligence ("AI"), machine learning, and related techniques. The control states that "[s]ystem and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data."[101] As a first challenge, the control says that, for personally identifiable information, "all sensitive details and content should be protected by removal or modification . . . ."[102] In practice, however, creating test sets that are resistant to re-identification may be technically difficult and expensive. Given the broad legal definition of what counts as personal data, it may not be feasible to select test data that entirely lacks personal data. Gathering data from across the organization, for better AI and other results, thus may violate localization requirements. As a related problem, as discussed in our TTP paper, limiting test data to each country reduces the ability of the defensive system to find statistically significant differences between signal (evidence of a cybersecurity risk) and noise.

**Control 15: Supplier relationships**.[103] This control addresses the common situation where an organization relies on an outside vendor. Localization in general will reduce the number and variety of providers that are available in the jurisdiction. For example, the locally available services may not have all of the cybersecurity features and quality that may be available in the global market. As discussed below in connection with third-party cybersecurity services, services that can be affected in this way include cloud services, software as a service, platform as a service, and infrastructure as a service.

**Control 16: Information security incident management**.[104] Detailed data is used at many stages of an organization's management of a breach or other security incident. Attackers who break into an organization's system are violating the law, and are unlikely to be stopped by concerns about transferring data across national borders. Defenders need to protect the organization's entire system — attackers may illegally enter anywhere in the system, and then seek to escalate privileges, by moving laterally and vertically to other parts of the system, including across borders.

To manage security incidents, Control 16 states, "[t]he organization should define and apply procedures for the identification, collection, acquisition and preservation of

[100] *Id.* at 62.
[101] *Id.*
[102] *Id.*
[103] *Id.* at 62–67.
[104] *Id.* at 67–71.

information, which can serve as evidence."[105] We highlight three examples where localization would impact an organization's response to a breach or other security incident.

First, by segmenting an organization's system, localization can make it more difficult to *detect* an intrusion. Intrusion detection seeks to identify anomalies, but account names, device identifiers, and other types of personal data could not be shared across the organization. Second, responding to incidents includes detailed *forensics*, seeking to understand as much as possible about the attack. Localization laws block the ability of an employee or forensics service to access relevant forensics information in the country with localization rules. Third, where detection, forensics, and other measures are degraded, *deterrence* is reduced.

**Control 17: Information security aspects of business continuity management**.[106] To respond to adverse situations, such as a crisis or disaster, the organization should use "personnel with the necessary authority, experience, and competence . . . ."[107] If only in-country personnel can access the system, which contains personal data, out-of-country personnel could not assist remotely during the crisis or disaster. Control 17.2 addresses redundancies, stating that "[i]nformation processing facilities should be implemented with redundancy sufficient to meet availability requirements."[108] This sub-control illustrates that localization would not only require data storage and back-up within the country, but also sufficient redundancy within the country to meet availability requirements.

**Control 18: Compliance**.[109] Control 18.2 calls for an independent review of information security, "[s]uch an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security."[110] 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. Personal data in one country would not be reviewable from another country, limiting testing and reducing the overall scope of the independent review.

### *2. Examples of Obstacles to Integrated Management Due to Data Localization*

By examining each control under ISO 27002, we have shown how localization can negatively affect 13 of the 14 relevant controls (excluding controls 1 to 4, which are introductory) — all except for Control 11, on physical and environmental security. This

[105] *Id.* at 70.
[106] *Id.* at 71–74.
[107] *Id.* at 72.
[108] *Id.* at 73.
[109] *Id.* at 74–78.
[110] *Id.* at 77.

control-by-control analysis shows the pervasive effect that hard localization laws have on an organization's cybersecurity management.

We draw some themes from this analysis. *One general result of localization is greater complexity*, to manage the network segregated by nation, and "complexity is the enemy of cybersecurity."[111] *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 a shift operation (24/7/365) 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 control-by-control analysis, we note 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.

1. Human resources.[112]
2. Customer/user support.[113]
3. Audit and compliance.[114]
4. Encryption.[115]
5. Sharding.[116]
6. Integrated management generally.[117]

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

---

[111] VMWare Editorial Board, *Complexity is the Enemy of Security: VMware Leaders Weigh in on How to Make Security Simpler, Faster and Smarter*, VMWARE SEC. & COMPLIANCE BLOG (June 29, 2021), 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; *see* ISO/IEC 27002:2013, *supra* note 20, at 43–45.

[112] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17 (Comment by Software and Information Industry Association; Comment by techUK; Comment by TechNet.).

[113] *Id.* (Comment by Confederation of Finnish Industries EK; Comment by Global Data Alliance; Comment by Adigital.).

[114] *Id.* (Comment by Workday, Inc.).

[115] *Id.* (Comment by Asia Cloud Computing Association; Comment by Information Technology Industry Council; Comment by American Chamber of Commerce in Spain; Comment by American Chamber of Commerce-Ireland; Comment by U.S. Mission to the EU; Comment by techUK.).

[116] *Id.* (Comment by Information Technology Industry Council.).

[117] *Id.* (Comment by Polish Chamber of Information Technology and Communications; Comment by Information Technology Industry Council; Comment by Palo Alto Networks; Comment by Peter Swire & DeBrae Kennedy-Mayo.).

### *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, protect privacy (the security of personal data), further "data sovereignty," and 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 privacy protection is to ensure a high level of data protection within the country. As Théodore Christakis wrote, "European calls in favor of data localization 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."[118]

The second argument for data localization, used in both democratic and non-democratic nations, is the issue of "data sovereignty." In Christakis's 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[.]'"[119] 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."[120]

Next, non-democratic countries' concern about data leaving the country appears to focus less on the protections for the data of individuals and more on national security implications.[121] For example, China requires a national security review of data that

---

[118] THÉODORE CHRISTAKIS, "EUROPEAN DIGITAL SOVEREIGNTY": SUCCESSFULLY NAVIGATING BETWEEN THE "BRUSSELS EFFECT" AND EUROPE'S QUEST FOR STRATEGIC AUTONOMY ii (2020); *see* Selby, *supra* note 26, at 218–19.

[119] CHRISTAKIS *supra*, note 118, at i.

[120] *Id.* at ii.

[121] *See* Selby, *supra* note 26, at 221–27; Chander & Lê, *supra* note 26, at 682–713. "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." PETER G. LEONARD ET AL., REGULATION OF CROSS-BORDER DATA TRANSFERS OF PERSONAL DATA IN ASIA 1, 6 (Clarisse Girot ed., 2018). *See* BUI NGOC SON, CONSTITUTIONAL CHANGE IN THE CONTEMPORARY SOCIALIST WORLD, (Oxford Univ. Press, 2020); *see* Jyh-An Lee, *Hacking into China's Cybersecurity Law,* 53 WAKE FOREST L. REV. 57, 90 (2018); *see* Rogier Creemers, *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century,* 26 J. CONTEMP. CHINA 85, 95 (2017).

leaves the country.[122] A second concern in non-democratic countries that have data localization requirements relates to data entering the country. These countries typically restrict the data that citizens can access.[123] The best-known example of this approach is the Great Firewall of China.[124]

The risks and benefits appear to vary considerably based on the size of the localized market. Consider the possibility of sharding,[125] specifically among multiple data centers or providing physically separate data centers for backup purposes. Large markets, such as China, may reach an efficient scale for these security controls.[126] By contrast, smaller markets may not be large enough to support even one world-class data center, much less provide an economic rationale for multiple, expensive data centers.[127]

For any restrictions on data transfers, there may also be mitigations that enable cybersecurity protections consistent with localization laws. For instance, secure multi-party computation and homomorphic encryption may enable cybersecurity-related sharing on encrypted data.[128] Such techniques are likely to become more important in the future, but currently, even within the most sophisticated organizations, there has been limited implementation even within the most sophisticated organizations. If such mitigations exist and are effective in protecting cybersecurity, they would reduce the negative effects of localization.

## 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 defines and analyzes the effects of localization on the cybersecurity services markets.

---

[122] *See* Daniel Cohen et al., *Impact of the New China Data Security Law for International Investors and Businesses,* AKIN (July 26, 2021), https://www.akingump.com/en/insights/alerts/impact-of-the-new-china-data-security-law-for-businesses-and-international-investors-1.

[123] Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 WORLD TRADE REV. 314, 348 (2020); Geoffery Hoffman, *Chapter 9: Cybersecurity Norm-Building and Signaling with China*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 187, 188 (Dennis Broeders & Bibi van der Berg eds., 2020).

[124] *See generally* Jyh-An Lee & 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); *see generally* Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State,* 30 J. DEMOCRACY 53, 55–56 (2019).

[125] *Database Sharding – System Design*, GEEKS FOR GEEKS (Oct. 21, 2014), https://www.geeksforgeeks.org/database-sharding-a-system-design-concept/.

[126] *See* Selby, supra note 26, at 225; *see* Patrick Spaulding Ryan et al., *When the Cloud Goes Local: The Global Problem with Data Localization,* 46 COMPUT., Dec. 2013, at 54, 57.

[127] *See generally* Rich Miller, *The Billion-Dollar Data Centers*, DATACTR. KNOWLEDGE (April 29, 2013), https://www.datacenterknowledge.com/hyperscalers/the-billion-dollar-data-centers.

[128] Anastasios Arampatzis, *Applications of Homomorphic Encryption and Secure Multi-Party Computation*, VENAFI (June 3, 2024), https://venafi.com/blog/applications-of-homomorphic-encryption-and-secure-multi-party-computation/; *see What is Homomorphic Encryption?,* IEEE DIGIT. PRIV., https://digitalprivacy.ieee.org/publications/topics/what-is-homomorphic-encryption? (last visited Jan. 9, 2025).

### *1. Defining the Cybersecurity Services Markets*

Definitions vary for categories of third-party services. A variety of terms describe these services, including cloud computing, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).[129] The definitions by Raza give a sense of the differences. He says, "SaaS leverages 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."[130] Next, "[c]loud 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 that developers can build upon and use to create customized applications."[131] In addition, "IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services."[132] That is, IaaS clients retain "complete control over the entire infrastructure."[133] These definitions of SaaS, PaaS, and IaaS suggest the range of ways that organizations rely on third-party services, including cybersecurity software.

*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 2022 for cybersecurity services is roughly $300 billion and is expected to grow to roughly $400 billion by 2027.[134] To the extent data localization impacts the provision of cybersecurity-related services, localization would affect this very large sector.

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

[129] Muhammad Raza, *SaaS vs. PaaS vs. IaaS: What's the Difference and How to Choose,* BMCBLOGS (Mar. 11, 2024), https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose.
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Cyber Security Market Size, Share, COVID-19 Impact & Industry Analysis*, FORTUNE BUS. INSIGHTS (Apr. 2023), https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165; Alexandra Borgeaud, *Size of the Cybersecurity Market Worldwide, from 2020 to 2030 (in Billion U.S. Dollars),* STATISTA (Aug. 30, 2023), https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/; Glob. Mkt. Insights Inc., *Cybersecurity Market to Hit $400 Bn by 2027: Global Marketing Insights, Inc.,* PR NEWSWIRE (June 29, 2021, 4:00 ET), https://www.prnewswire.com/news-releases/cybersecurity-market-size-to-hit-400-bn-by-2027-global-market-insights-inc-301321491.html.

more narrowly defined.[135] Among cloud providers, the top three are Amazon, Google, and Microsoft.[136]

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 administrators.

*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. Managers of large organizations understand 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 an important and increasing reason to seek assistance from third-party service providers. With a shortage of cybersecurity experts and limited budgets, SMEs often lack the in-house capability to implement and update high-quality cybersecurity measures.[137] The epidemic of ransomware attacks against small municipalities and other smaller organizations is evidence of the need for SMEs to get third-party assistance to manage cybersecurity.[138] Thus, the impact is disproportionate as SMEs do not have the same resources to recruit, hire, train, and retain relevant cybersecurity expertise in comparison to large multinationals.

---

[135] *See* Laurens Cerulus, *France Wants Cyber Rule to Curb US Access to EU Data*, POLITICO (Sep. 13, 2021, 5:32 PM), 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 (Oct. 12, 2021), https://techhq.com/2021/10/in-europe-big-tech-providers-are-at-the-mercy-of-data-sovereignty/.

[136] Shelby Hiter, *Cloud Computing Market 2021*, DATAMATION (Aug. 13, 2021), https://www.datamation.com/cloud/cloud-computing-market/; Laurens Cerulus, *Big Tech Cries Foul Over EU Cloud-Security Label,* POLITICO (June 14, 2022, 3:65 PM), https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/; *Leading Cybersecurity Vendors by Market Share Worldwide from 2017 to 2020. Technology & Telecommunications, Software,* STATISTICA, https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share/ (last accessed Nov. 7, 2023); *see Managed Security Services Market by Service Type (Managed IAM, MDR, Managed SIEM and Log Management), Type (Fully Managed & Co-Managed), Security Type (Network, Cloud, Endpoint, Application), Organization Size, Vertical & Region- Global Forecast to 2027,* MKT. BY MKT. (Nov. 2022), https://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html; Chander & Lê, supra note 26, at 679–80.

[137] *Cyber Security Market Size, Share & COVID-19 Impact Analysis, 2021-2028*, FORTUNE BUS. INSIGHTS (Mar. 2021), https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

[138] Andy Castillo, *Ransomware Attacks Highlight Need for Adequate Cybersecurity*, AM. CITY & CNTY. (July 7, 2021), https://www.americancityandcounty.com/2021/07/07/ransomware-attacks-highlight-need-for-adequate-cybersecurity/; Sam Greengard, *Why are SMBs Under Attack by Ransomware,* CSO (June 14, 2021), https://www.csoonline.com/article/570855/why-are-smbs-under-attack-by-ransomware.html; Lisa Thompson & Hage Hodes, *Practical Measures for Local Government to Avoid Ransomware,* ICMA BLOG (June 4, 2021), https://icma.org/blog-posts/practical-measures-local-government-avoid-ransomware.

*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 comply with both regimes, and large companies may be early targets for enforcement actions.[139] 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 limited geographies, and so cannot remotely assist clients in other countries.

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

There are categories of risk from limits on cybersecurity services, with the risk depending on the scope and details of those restrictions.

*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

[139] Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975, 1979 (2005).

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 (and their sub-providers) would encounter the same obstacles in seeking to assist the organization achieve integrated management.

*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 predictably fall.

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

1. State-of-the-art cybersecurity services.[140]
2. Global cloud service providers.[141]
3. Global supply chains.[142]
4. Information security talent outside of the Single Market.[143]
5. Resolution of bugs or security issues in relation to personal data hosted.[144]
6. Packet inspection.[145]
7. Monitoring for cyber threats.[146]
8. Threat intelligence and threat prevention.[147]

### *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

[140] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17 (Comment by Chamber of Commerce of the United States of America; Comment by American Chamber of Commerce in Czech Republic; Comment by Slovak Alliance for Innovative Economy (SAPIE).).
[141] *Id.* (Comment by BSA The Software Alliance; Comment by American Chamber of Commerce in Spain.).
[142] *Id.* (Comment by Vodafone.).
[143] *Id.* (Comment by Chamber of Commerce of the United States of America.).
[144] *Id.* (Comment by Confederation of Swedish Enterprise; Comment by American Chamber of Commerce in Slovenia; Comment by BSA The Software Alliance;Comment by Confederation of Industry in the Czech Republic;Comment by Information Technology Industry Council.).
[145] *Id.* (Comment by Confederation of Swedish Enterprise; Comment by American Chamber of Commerce in Slovenia; Comment by BSA The Software Alliance; Comment by Confederation of Industry in the Czech Republic; Comment by Information Technology Industry Council.).
[146] *Id.* (Comment by Palo Alto Networks.).
[147] *Id.* (Comment by Software and Information Industry Association; Commnet by Palo Alto Networks).

a reason to support localization.[148] Localization thus may help create national champions for cybersecurity and increase a country or region's digital sovereignty.[149]

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, 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 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 comes 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.

The risk/benefit analysis may be factually different for China. China already has a large internal market, with limited dependence on third-party cybersecurity services from outside of the country. By contrast with countries that currently import many cybersecurity services, additional localization requirements in China may not affect the status quo nearly as much. Strict localization requirements, however, would continue to create obstacles to integrated management of firms (Chinese-based or otherwise) that operate both inside and outside of China.

## D. Obstacles to Information Sharing

A mantra in cybersecurity policy discussions has often been that there should be more information sharing.[150] One obvious effect of data localization is to reduce information sharing across borders, for the scope of data covered by the localization requirement.

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.

---

[148] Selby, *supra* note 26, at 213–232; Chander & Lê, supra note 26, at 690.
[149] Lokke Moerel, *The Ebb and Flow of Trans-Atlantic Data Transfers: It's the Geopolitics, Stupid,* FUTURE OF PRIV. F. (Apr. 4, 2022), https://fpf.org/blog/the-eb-and-flow-of-trans-atlantic-data-transfers-its-the-geopolitics-stupid.
[150] S. Norton, *Former NSA Director: Better Information Sharing Needed on Cybersecurity*, WALL ST. J. (Sept. 30, 2014), https://www.wsj.com/articles/BL-CIOB-5467.

For one of the authors (Swire), the topic of information sharing, cybersecurity, and privacy has been the subject of two previous research projects. One project analyzed the conditions where the benefits of disclosure to the defender are greater than the risks of disclosure to the attackers.[151] The second project analyzed information sharing in the period after the attacks of September 11, 2001. To consider both privacy and security, the author proposed a "Due Diligence Checklist for a Proposed Information Sharing Program."[152] Taking the two papers together, the mantra of improving cybersecurity through information sharing will often be true. Such findings, however, are subject to the constraints discussed in the two earlier papers.

### *1. Examples of Cybersecurity Risks for Information Sharing Due to Data Localization*

A pervasive tool in cybersecurity is the sharing of information with other parties to enhance defense mechanisms. The importance of information sharing has led to important institutions such as CERTs (computer emergency response teams) and ISACs (information sharing and analysis centers), as well as the enactment of laws designed to facilitate information sharing, such as the Cybersecurity Information Sharing Act of 2015. *When data localization blocks information sharing, it jeopardizes the effectiveness of many established and possible future institutional methods for information sharing.*

As discussed above, important cybersecurity services include monitoring for cyberattacks, threat analysis, and threat prevention. These services often include significant information sharing, including data about IP addresses associated with cyberattacks. *Obstacles to the international provision of such cybersecurity services are also obstacles to information sharing practices.*

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 cybercrimes.[153] Due to the substantial portion of cyberattacks originating in different countries, restrictions on information sharing impede collaboration and cooperation in investigating cyberattacks. Moreover, the advent of cloud computing has facilitated the "globalization of criminal evidence" — investigations of crimes beyond

[151] Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?,* 3 J. TELECOMM. & HIGH TECH. L. 163, 197 (2004); Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1338 (2006).
[152] Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL L. REV. 951, 952 (2006).
[153] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17 (Comment by Interactive Advertising Bureau Poland; Comment by Software and Information Industry Association; Comment by U.S. Mission to the EU; Comment by Centre for Information Policy Leadership; Comment by CrowdStrike.).

cybercrime are frequently constrained when data cannot be transferred from other countries.[154]

2. *Forensic investigations of cyberattacks*, including DDOS, malware, phishing attempts, and ransomware incidents, play a crucial role in identifying and mitigating breaches.[155] These investigations often entail extensive forensic investigation and analysis. However, because attackers often intentionally traverse international borders to evade detection, forensic investigations can become significantly less effective in the absence of cross-border information sharing.
3. *Global training of datasets.*[156] Cybersecurity increasingly relies on AI and other automated techniques to detect and respond to cyberattacks. However, data localization reduces the range of data available within any single country, hindering the creation of comprehensive datasets necessary to train for such defensive measures. Furthermore, data localization prevents detection of potentially useful patterns that may only be detected from data sourced across multiple countries.
4. *Anti-fraud and anti-abuse.*[157] Information is pervasively shared to reduce the incidence and costs of fraud, along with other forms of abuse like child sexual abuse material ("CSAM"). Data localization cuts off information sharing crucial for fraud detection and prevention, potentially leading to increased criminal activity, both online and offline. A specific risk associated with localization is that perpetrators of fraud or abuse can operate across different geographic regions without their identity being known to potential victims in other regions.

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

---

[154] Peter Swire et al., *The Globalization of Criminal Evidence,* IAPP (Oct. 16, 2018), https://iapp.org/news/a/the-globalization-of-criminal-evidence/.

[155] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17 (Comment by Palo Alto Networks; Comment by CrowdStrike.). 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 (Oct. 14, 2021), 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. DEP'T OF STATE (Oct. 15, 2021), https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative.

[156] *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, *supra* note 17 (Comment by Interactive Advertising Bureau Poland.).

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

### *2. Possible Benefits of Localization and Mitigation of Its Risks*

Some countries may wish to have obstacles to information sharing, especially to reduce surveillance by the intelligence agencies of foreign countries.[158] In response, we note that numerous types of information sharing discussed above have important benefits but little or no connection to the 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 multilateral efforts are underway to develop principles for government access to data held by private actors including initiatives within the Organization for Economic Cooperation and Development and the Global Privacy Assembly.[159] These efforts are directly aimed at reducing the risk from surveillance, especially from other democratic countries. Third, the discussion above has provided insights from previous research efforts regarding instances when data sharing indeed is justified. In short, implementing a blanket ban on data sharing across borders would appear over-broad.

## VI. Conclusion

Hard data localization, which blocks categories of transfers, has numerous effects on an organizations' ability to defend against cyberattacks. In some ways, expert commentators have already been aware of the problem, as shown by the numerous comments on the EDPB Guidance that mention the possible effects on cybersecurity. Our research has drawn on these comments as a rich source of examples of possible problems. Additionally, 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 proposed a new organizing framework to comprehend the effects of data localization, focusing on its impacts within an organization, across organizations with payment, and across organizations without payment. First, within an organization, data localization creates many obstacles to the integrated management of cybersecurity risk, affecting 13 of the 14 ISO 27002 controls, along with additional sub-controls. Second, when an organization pays for third-party cybersecurity services,

---

[158] Selby, *supra* note 26, at 213–232; Ross Anderson, *Post-Snowden: The Economies of Surveillance*, LIGHT BLUE TOUCHPAPER (May 27, 2014), https://www.lightbluetouchpaper.org/2014/05/27/post-snowden-the-economics-of-surveillance/.

[159] *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) (Dec. 2020), https://web-archive.oecd.org/2021-10-26/575438-trusted-government-access-personal-data-private-sector.htm; D. Williams, *Reckoning with Cyberpolicy Contradictions in Great Power Politics,* BROOKINGS TECHSTREAM (Oct. 12, 2021), https://www.brookings.edu/techstream/reckoning-with-cyberpolicy-contradictions-in-great-power-politics; *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*, GLOB. PRIV. ASSEMBLY (Oct. 2021), https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf.

data localization creates numerous and severe obstacles to cybersecurity protection, in the rapidly growing market for such services. Perhaps most generally, localization will isolate a country from the state-of-the-art cybersecurity measures. Attackers will thus be incentivized to target organizations in localized regions where access to effective cybersecurity services is often limited. Third, where an organization does not pay third parties, the important category of "information sharing" would be significantly impacted by restrictions on data transfer.

This article on the organizational effects of localization complements our current paper on "Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures." That paper organizes its analysis around the effects of localization on technological measures such as pen testing, privilege escalation, and threat hunting.

With that said, this paper explains numerous significant reasons why hard data localization poses risks to cybersecurity. We believe that these risks should be explicitly addressed in future debates regarding the advisability of data localization, through at least three methods. First and most generally, we recommend that cybersecurity experts and government agencies thoroughly examine the risks detailed in this paper. For example, consider what types of third-party services might become unavailable due to localization, along with the associated increased risk. Second, if a general localization regime is in place, policymakers can consider creating exceptions that encompass concepts of necessity and proportionality in cases where a factual showing of cybersecurity risk exists. Third, the cybersecurity risks stemming from localization, including their effects on individuals, corporations, and national security, should be analyzed together with any claimed benefits. The claimed benefits may include reduced access by adversary governments and other actors seeking data held outside of the country. Regardless of the actual risks associated with data transfer, it seems irrational to solely focus on potential benefits from restricting data flows while disregarding known, probable, and substantial cybersecurity risks. In sum, until and unless proponents of localization address these concerns, scholars, policymakers, and practitioners have compelling reasons to expect significant cybersecurity harms resulting from hard localization requirements.

## VII. Acknowledgments

The authors presented an earlier version of the paper at the 2021 Cybersecurity Law and Policy Scholars Conference and thank the attendees for their feedback, as well as comments from Arnaud David and Eric Grosse. The authors thank Nathan Lemay for research on this project.

## VIII. Funding

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.