**Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data**

# "Five Concerns About Hard Data Localisation Within the European Union"

**By Peter Swire[1] & DeBrae Kennedy-Mayo[2]**

These comments set forth five concerns, based on our ongoing research, about the effects of data localisation. Relatively few writers have explicitly called for hard data localisation within the European Union. Nonetheless, expert European commentators have concluded that the November 10 documents from the European Data Protection Board would apparently have the effect of hard data localisation.[3]

We are U.S. academics who have previously studied cross-border data flows, including the effects of data localisation. In conjunction with the Cross-Border Data Forum, we are currently engaged in a substantial research project on data localisation. We plan to provide further research results as they become available.

As U.S. lawyers, we do not seek to offer interpretations of European Union law. Instead, we provide these comments as potentially useful descriptions of the effects of hard data localisation. We have read, such as in the writings of Professor Théodore Christakis, that the actual effects on data flows may be relevant to European Union legal concepts. For instance, practical effects of data flows may be relevant to judging when processing of personal data is necessary and proportionate.[4]

Based on our work to date, we offer the following five areas of concern about the effects of hard data localisation:

1. **Previous Research Shows Numerous Major Data Flows, Beyond Digital Platforms, that Would Be Affected by Hard Data Localisation.**

2. **Previous Research Shows Technical Obstacles to Providing Online Services in a Regime of Hard Data Localisation.**

3. **Strategies for Localising Data in the EU Work Less Well When Other Jurisdictions Also Require Data Localisation.**

4. **Seemingly Simple and Lawful International Transfers May Include Background Processing That May Not Be Consistent With Hard Data Localisation.**

5. **Hard Data Localisation May Create Cybersecurity, Anti-fraud, and Related Risks.**

## 1. Previous Research Shows Numerous Major Data Flows, Beyond Digital Platforms, that Would Be Affected by Hard Data Localisation.

The most detailed examination of flows of personal data out of Europe, of which the authors are aware, remains the book that one of the authors - Peter Swire - wrote with Robert Litan in 1998, called NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE.[5] The book catalogues roughly 40 categories and sub-categories of significant data flows from the EU, with the focus especially on flows to the United States. Many types of data flows are the same as in 1998, but there are important new categories of data flows, perhaps most notably for cloud computing, where the personal data of individuals is often stored, processed, and/or accessed in a different country.[6]

The publisher, the Brookings Institution, has recently made the **full text of the book available for free download** at https://www.brookings.edu/book/none-of-your-business/. Appendix 1 to this document provides the table of contents for Chapters 5 to 7, to indicate a list of sectors and types of data flows where hard data localisation may have significant effects, often to limit transfers. To date, much of the focus in commentary within the EU has been on data flows concerning the largest digital platforms. **Appendix 1 shows numerous effects of hard data localisation, beyond the largest digital platforms.**

We highlight one area for particular attention. **The possible disruption of data flows could include pharmaceuticals research**, which would be especially important to consider **during the COVID pandemic**, when sharing of personal data is so important concerning the safety and efficacy of vaccines and treatments as well as other medical information.[7]

## 2. Previous Research Shows Technical Obstacles to Providing Online Services in a Regime of Hard Data Localisation.

We highlight two previous studies, written by technical experts, that show technical obstacles to providing online services in a regime of hard data localisation. In addition, we explain the need for further research on the extent to which traffic sent from one user to another, within the same country, actually routes through one or more different countries.

The first paper is by research engineer Dillon Reisman, who presented his results at a 2017 conference at Georgia Tech that was sponsored, among others, by the European Union's Erasmus+ Program.[8] The conference was part of the authors' work leading the Georgia Tech Cross-Border Requests for Data Project,[9] which has now been included in the ongoing work of the Cross-Border Data Forum.[10]

Reisman published "Where Is Your Data, Really?: The Technical Case Against Data Localisation."[11] **Reisman identified the following technical obstacles to providing online services if hard data localisation is in place:**

1. Your data might be stored in edge caches across borders.
2. Your data might be replicated for load balancing.
3. Your data might be "sharded" across multiple machines in multiple data centers.
4. Your data might be backed up to multiple locations in case of failure.

5. Your data might be made accessible to engineers in different countries for maintenance and de-bugging.
6. Your data might be processed in batches at a central location, to add features such as search or artificial intelligence.
7. Your data might be processed to generate "derived data."

As specific points, Reisman explained that "data can live ephemerally, in many copies and in many places. Some of our most important Internet applications, from search functions to communications, rely on those places being across a national border." For tech companies, Reisman discussed the need for data to be accessible to employees – who may be located in different jurisdictions – in order to maintain these Internet applications, to ensure that processing occurs, and to provide support to users.

The second paper is by now-Professor Jonathan Mayer, of the Department of Computer Science at Princeton University. In his 2013 paper called "The Web is Flat" Mayer examined what he called the "international referrer" issue.[12] Mayer wrote: "A person within the United States may be reading a webpage that looks, and is, as American as apple pie. But that webpage can pull in dozens of unexpected sources." He adds: **"If just one of those third parties is international," the user's personal data will go outside of the user's country. Mayer tested 2,500 popular websites and found "international referrers are pervasive."** For U.S. users, he concluded: "So much for a bright line dividing the domestic and international Web." Given the large number of web services that exist in the U.S. and other third countries, it would seem likely that individuals in the EU would encounter pervasive international referrers as well – **current websites "pervasively" refer browsing activity outside of the EU, so hard data localisation would appear to entail pervasive re-design and re-sourcing for websites accessed by EU users.**

**One topic for further research is the extent to which traffic sent from one user to another, within the same country, actually routes through one or more different countries.** The simple idea is that Internet communications do not travel in a straight line from two users, such as Alice to Bob. Instead, as explained in an introductory lesson by Khan Academy, "computers split messages into packets and those packets hop from router to router on their way to their destination."[13] **Currently, there is no infrastructure in place to ensure that packets sent from within the EU route only through the EU or that all packets sent from the EU are encrypted.**[14] As the Internet Society explains in its examination of data localisation, "even if data is located in one country, the transmission path may cross national borders for resilience or performance reasons."[15]

As one additional point about routing, a 2017 paper by computer scientist Peter Mell and others examines "information exposure," defined as 'the extent to which communications between pairs of countries are exposed to other countries."[16] The paper establishes that countries that are "well connected" – that have more connections to the global Internet – face a greater likelihood of such information exposure. By contrast, a country such as China that limits exposure to the global Internet has a lower likelihood that its communications will pass through other countries as a result of the Internet Protocol's routing structure. **The Mell paper raises the possibility that effective blocking of packets from going outside of the EU, at a technical level, may require regulatory limits on transfers more similar to the current Chinese approach.**

## 3. Strategies for Localising Data in the EU Work Less Well When Other Jurisdictions Also Require Data Localisation.

For a business headquartered in the EU, one appealing strategy, in the face of hard data localisation, may be to centralise data processing in the EU. Under this strategy, for instance, the company could keep human resources records within the EU to the maximum extent feasible. Processing then would remain under EU data protection rules while it stayed in the EU. Transfers to third countries could be relatively uncommon, perhaps enabling the company to rely on derogations, or at least reducing the amount of possibly unlawful transfers. **Indeed, under this approach, companies based either inside or outside of the EU could decide to shift their human resources and other records into the EU, so that corporate decisions could be made based on the data that is allowed to come into the EU.** Under this approach, centralising data processing in the EU may therefore aid in compliance and reduce the risk of enforcement actions.

**This EU-based architecture, however, works less well when other jurisdictions also require data localisation.** Continuing with the human resources example, the other jurisdictions may limit transfers back to EU headquarters. For an example involving customer records, such as for e-commerce purchases from outside of the EU, the customer records may also need to be stored in the other jurisdiction. In each of these simple examples, it may not be possible to meet the data localisation requirements of both the EU and the other jurisdiction.

**Data localisation outside of the EU is already significant, and may grow substantially if the EU imposes hard data localisation.** First, nations, such as China, already have a hard data localisation regime, and China is a leading trading partner for some Member States. Second, other important trading partners, such as India, are seriously considering data localisation regimes. Third, GDPR and other aspects of EU data protection law have been widely copied by nations around the world. If the EU interprets its regime to require data localisation, other countries could interpret their own "adequacy" and other provisions to require data localisation as well; moreover, the ability of the EU to achieve free trade goals generally may be reduced if the EU becomes a leading adopter of limits on cross-border economic activity.

**In conclusion, to the extent that more jurisdictions follow an EU approach for data localisation, then strategies for localising personal data within the EU would work less well than may have been apparent to date.**

## 4. Seemingly Simple and Lawful International Transfers May Include Background Processing That May Not Be Consistent With Hard Data Localisation.

Another theme in our ongoing research is that apparently simple and lawful data flows may not be so simple in practice. Consider an individual in the EU booking a hotel room in the U.S., an example provided by the prominent privacy organisation noyb.[17] The contemplated data flow involves an informed choice by an EU person, such as Alice, to have her personal data go to the U.S. This data flow would, according to the example, rely on one or more of the Article 49 derogations.

**Along with this direct booking request for a hotel room, there likely would be a number of other data flows, occurring in the background and often not visible to Alice.** We provide several examples here. In doing so, we do not propose a legal conclusion about exactly which of

these may be lawful under Article 49 derogations; instead, the point is to illustrate that there is often background processing to accompany a seemingly simple customer request:

1. **Existing customer records.**
    a. Alice may have user preferences, such as for a double or king-sized bed.
    b. Alice may be part of a loyalty program, and she wishes to get "credit" for the nights she stays in the U.S. hotel. The hotel may wish to inform her that she can get a free night if she stays one extra night.
    c. Alice may have a preferred customer status, based on her purchases in the EU, and the U.S. hotel should give her a free breakfast or other benefits.
    d. Alice may wish to receive coupons or other offers from other companies, such as for car rentals or discounted admission to tourist attractions. Such offers may be based on personal data processed in the EU.
2. **Payment information.**
    a. Travel agents or other companies in the EU may receive payment, in whole or in part, and then communicate payment status to the U.S. hotel. Updates on booking status may flow back and forth if Alice changes her travel plans once in the U.S.
    b. Alice may have a credit card or other method of payment on file in the EU, and wish to use it easily in the U.S.
    c. Alice may have a branded credit card, such as an airline miles card, so personal data about her trip goes to the airline as well as the credit card company.
    d. There may be regulatory requirements that would trigger additional cross-border flows. As one example, if Alice preferred to pay in cash for an extended visit, that may trigger requirements under anti-money laundering laws, leading to follow-up investigation and access to personal data from the EU.
3. **Accounting and anti-fraud.**
    a. The U.S. hotel and relevant EU companies all have accounting obligations, so personal data may be exchanged EU/U.S. as part of routine accounting activities.
    b. Accounting also applies to each step of the payments system, with EU actors sharing sufficient data with U.S. actors to ensure accurate entry and accounting for the payment transactions.
    c. When Alice arrives at the hotel, there may be authentication information received from the EU to verify her identity.
    d. Along with authentication information, an EU company may provide personal data in determining the maximum bill Alice can incur at the U.S. hotel.
    e. Alice may have a history with the hotel chain in the EU of canceling reservations at the last minute, so the U.S. hotel may decide to make the reservation non-refundable.

**This list is provided by way of example – a seemingly simple and one-time transaction (booking a hotel room) – may be accompanied by multiple, routine, and ongoing transfers of personal data.** Consistent with generally hard data localisation, there may be ways to gain consent that meets EU requirements, or otherwise structure the hotel booking to meet Article 49 derogations or have some other lawful basis. The point, however, is that **one should consider background processing before reaching any conclusion about whether a seemingly simple transaction is lawful.**

## 5. Hard Data Localisation May Create Cybersecurity, Anti-fraud, and Related Risks.

Hard data localisation may create risks for cybersecurity, anti-fraud, and related prudential activities. **The basic idea is that information can be an important component of defending against and responding to cyber-attacks. The respected Internet Society has stated, for instance, that "Cybersecurity may suffer as organisations are less able to store data outside borders with the aim of increasing reliability and mitigating a wide variety of risks including cyber-attacks and national disasters."[18]**

Some reasons data localisation may harm cybersecurity include the following:

1. The general concern that reduction in available information will increase the risks from cyber-attacks.
2. It may be more costly to implement and maintain state-of-the-art tools, across different localisation regions.
3. The loss of redundant storage increases the risk of data loss or network outage in the case of a hardware malfunction or natural disaster.
4. Options for distributed storage solutions, which often assist in deploying privacy, integrity, and counter-intrusion protocols on networks, would be less available to data controllers.

We hope to provide greater detail about effects on cybersecurity in future research. At this time, we simply point to the topic as one worth considering as part of the overall effects of hard data localisation.

## APPENDIX 1

**Table of Contents for Chapters 5 to 7 of the 1998 book entitled NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE[1]**



[1] Peter Swire & Robert Litan, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (Brookings 1998), https://www.brookings.edu/book/none-of-your-business/. Thanks to permission from its publisher, the Brookings Institution, that book is now downloadable from the Brookings website. The link to the PDF of the book is located on the left side of the webpage.

[1] Peter Swire is the Elizabeth and Tommy Holder Chair and Professor of Law and Ethics in the Scheller College of Business at the Georgia Institute of Technology. He is senior counsel with the law firm of Alston & Bird, and Research Director of the Cross-Border Data Forum. The comments in this document should not be attributed to the Cross-Border Data Forum or any client. The authors thank Paul Greaves, Nathan Lemay, and Yung Shin Van Der Sype for research assistance on these issues.

In 1998, the Brookings Institution published Swire & Litan, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE. In 1999, Swire was named Chief Counselor for Privacy in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy. Swire was the lead White House privacy official during negotiation of the EU/U.S. Safe Harbor.

After the Snowden revelations, Swire served as one of five members of President Obama's Review Group on Intelligence and Communications Technology, making recommendations on privacy and other reforms for the U.S. intelligence community. In 2015, the International Association of Privacy Professionals awarded Swire its annual Privacy Leadership Award. In 2016 he was an expert witness in the Irish trial for *Schrems v. Facebook*, and submitted testimony of over 300 pages describing the legal safeguards for the U.S. intelligence community's use of personal data.

In 2018, Swire was named an Andrew Carnegie Fellow for his project on "Protecting Human Rights and National Security in the New Age of Data Nationalism." In 2019, the Future of Privacy Forum honored him for Outstanding Academic Scholarship.

[2] DeBrae Kennedy-Mayo is a research faculty member in the Scheller College of Business at the Georgia Institute of Technology. She is also a senior fellow with the Cross-Border Data Forum. Swire and Kennedy-Mayo are the co-authors of the 2020 edition of the International Association of Privacy Professionals book entitled U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS. In this book, Kennedy-Mayo is the co-author (along with an EU attorney) of the chapter focused on the GDPR.

[3] Professor Théodore Christakis, in his European Law Blog articles, reached the following conclusions about the two documents issued by the European Data Protection Board on November 10, "Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data" and "Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures" ("draft Recommendations"):

1. "Third countries might rarely if ever meet" the requirements set forth in the European Essential Guarantees. He states, except for the small number of countries with an adequacy decision, "few other countries might be considered as offering a protection 'essentially equivalent' to that offered by EU law."
2. "The EDPB's guidance clearly indicates that no data transfer should take place to non-adequate/non-essentially equivalent countries unless the data is so thoroughly encrypted or pseudonymised that it cannot be read by anyone in the recipient country, not even the intended recipient."

The three articles by Professor Christakis are: "'*Schrems III*'? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)," European Law Blog (13 Nov. 2020), https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/; "'*Schrems III*'? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)," European Law Blog (16 Nov. 2020), https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/; "'*Schrems III*'? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)," European Law Blog (17 Nov. 2020), https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3.

[4] *Id.*

[5] Peter Swire & Robert Litan, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (Brookings 1998), https://www.brookings.edu/book/none-of-your-business/. Thanks to permission from its publisher, the Brookings Institution, that book is now downloadable from the Brookings website. The link to the PDF of the book is located on the left side of the webpage.

[6] Several current reports are also available that provide useful discussion of the impacts of cutting off data, including two reports on *Schrems II* as well as one report focusing on standard contractual clauses. *See* "*Schrems II* Impact Survey Report," Joint Report by DigitalEurope, BusinessEurope, European Round Table for Industry, & European Automotive Manufacturers Association (26 Nov. 2020), https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/; Nigel Cory, Daniel Castro, & Ellysse Dick, "'*Schrems II*': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation," Information Technology & Innovation Foundation (3 Dec. 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic; Nigel Cory, Ellysse Dick, & Daniel Castro, "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade," Information Technology & Innovation Foundation (17 Dec. 2020), https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade?mc_cid=54d797e40f&mc_eid=83842a0eb3.

[7] Chapter 7 looks at "other sectors with large transborder activities."

[8] "Surveillance, Privacy and Data across Borders: Transatlantic Perspectives," Conference hosted by the Center for European and Transatlantic Studies, the Institute for Information Security & Privacy at Georgia Tech, and the Scheller College of Business at Georgia Tech as well as supported by the European Union's Erasmus+ Program and the William and Flora Hewlett Foundation (18 April 2017), https://cets.gatech.edu/news-2/surveillance-privacy-and-data-across-borders-transatlantic-perspectives/.

[9] Cross-Border Requests for Data Project, Institute for Information Security & Privacy at Georgia Tech, https://iisp.gatech.edu/cross-border-data-project.

[10] Cross-Border Data Forum, https://www.crossborderdataforum.org.

[11] Dillon Reisman, "Where is Your Data Really?: The Technical Case Against Data Localisation," Lawfare (22 May 2017), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.

[12] Jonathan Mayer, "The World is Flat," Web Policy (30 Oct. 2013), http://webpolicy.org/2013/10/30/the-web-is-flat/. Mayer wrote in 2013, and his paper expressed concern about excess surveillance by the U.S. National Security Agency. At the request of the Belgian Data Protection Agency, Swire testified on 24 actions that the U.S. took after the Snowden revelations to reform surveillance laws and practices, and improve privacy safeguards. Peter Swire, "Chapter 3: The U.S. Has Taken Multiple and Significant Actions to Reform Surveillance Laws and Programs Since 2013," U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013 (18 Dec. 2015), https://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf.

[13] Pamela Fox, "Routing with Redundancy: Internet Routing Protocol," Unit: The Internet, Course: Computers and the Internet, Khan Academy, https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:routing-with-redundancy/a/internet-routing.

[14] *See* Use Case 3: Encrypted data merely transiting third countries, Annex 2: Examples of Supplementary Measures, European Data Protection Board Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (adopted on 10 November 2020), https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

[15] "Internet Way of Networking Use Case: Data Localisation," Internet Society (30 Sep. 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.

[16] Peter Mell, Assane Gueye, & Christopher Schanzle, "Quantifying Information Exposure in Internet Routing," IEEE (2018), https://ieeexplore.ieee.org/document/8456105.

[17] The example comes from "Next Steps for Users & FAQs": "Which data transfers are still legal? Under Article 49 GDPR, some 'necessary' transfers are still legal in any circumstance (e.g. when you book a hotel in the US and the booking is sent to the US hotel). It is still legal to transfer data when you were informed about US laws and you have explicitly and freely agreed to it. You must be able to withdraw this consent at any time, without negative consequence. You can also always send you own data to the US (if you wish to directly use a provider that is only in the US)." FAQs for Users, Next Steps for Users & FAQs, noyb (24 Jul. 2020), https://noyb.eu/en/next-steps-users-faqs.

[18] "Internet Way of Networking Use Case: Data Localisation," Internet Society (30 Sep. 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.