EXAMINING NATIONAL PRIVACY LAWS IN THE CONTEXT OF INTERNATIONAL
TRADE

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Public Policy
in Public Policy

By

Caitlin T. Chin, B.A.

Washington, D.C.
April 11, 2020

Copyright 2020 by Caitlin T. Chin
All Rights Reserved

EXAMINING NATIONAL PRIVACY LAWS IN THE CONTEXT OF INTERNATIONAL TRADE

Caitlin T. Chin, B.A.

Thesis Advisor: Andrew S. Wise, Ph.D.

ABSTRACT

In recent years, multiple government officials, members of civil society, industry representatives, and academic scholars have suggested that a direct relationship exists between a country's data privacy framework and international trade prospects. However, quantitative research in this field is still nascent. Therefore, this thesis explores the relationship between countries' data privacy laws and annual commercial services exports and imports. I hypothesize that a positive correlation exists between privacy laws and international trade: I predict that countries or territories with stronger national privacy laws are likely to see higher levels of commercial services exports and imports, holding constant various control factors. Using demographic and international trade data from the World Bank and the World Trade Organization, I adopt linear and fixed-effects regression models to analyze national data privacy frameworks from 202 countries or territories between 2005 and 2018. I find that the results of this study generally support my hypothesis, although I underscore the limitations of these findings, including missing data and uncontrollable confounding variables. Finally, I offer conclusions and policy recommendations based on my preliminary analysis and offer support for further research into this topic.

ACKNOWLEDGEMENTS

I dedicate my thesis to Cameron Kerry, whose thought leadership on privacy inspires my work, Andrew Wise, for his feedback and mentorship throughout my research process, my mother, Paula Chin, for her unending encouragement, and everybody else who helped along the way.

Any errors or omissions in this thesis are my own.

Many thanks,
Caitlin T. Chin

TABLE OF CONTENTS

I. Introduction and Background	1
II. Literature Review	4
A. Compliance Costs	5
B. Interoperability of National Privacy Laws	6
C. Data Adequacy Requirements	6
D. Consumer Trust in Companies	8
E. Diplomacy and Privacy Values	9
F. Continuing the Discussion	9
III. Theoretical Model	11
IV. Empirical Model	12
V. Data	14
A. Independent Variable: Privacy Laws	14
B. Dependent Variable: International Trade	15
C. Control Variables	16
VI. Results	20
VII. Conclusion and Policy Recommendations	28
Appendix A: International Privacy Legal Resources	30
Appendix B: Additional Control Variables	36
Bibliography	39

LIST OF TABLES

Table 1. Descriptive Statistics.....	19
Table 2. Linear and Fixed-Effects Regression Models of National Privacy Laws and Demographic Variables on Log Commercial Services Exports (2005-2018)	21
Table 3. Linear and Fixed-Effects Regression Models of National Privacy Laws and Demographic Variables on Log Commercial Services Imports (2005-2018)	24
Table 4. Linear and Fixed-Effects Regression Models of Maximum Monetary Penalties and Demographic Variables on Log Commercial Services Exports and Imports (2005-2018)	26
Table 5. Linear and Fixed-Effects Regression Models of National Privacy Laws and Demographic Variables on Log Commercial Services Exports (2005-2018)	36
Table 6. Linear and Fixed-Effects Regression Models of National Privacy Laws and Demographic Variables on Log Commercial Services Imports (2005-2018)	37
Table 7. Linear and Fixed-Effects Regression Models of Maximum Monetary Penalties and Demographic Variables on Log Commercial Services Exports and Imports (2005-2018)	38

I. INTRODUCTION AND BACKGROUND

In the United States and around the world, there are economic interests in both protecting data privacy and facilitating cross-border data flows. However, these two are sometimes at odds: most countries regulate and enforce data privacy rules in different ways, and as a result, any single online transaction could be subject to multiple legal frameworks. Furthermore, some data privacy frameworks may legally restrict cross-border data transfers. In this thesis, I study the relationship between national data privacy frameworks and international trade. My hypothesis is that the enactment of strong national privacy laws is positively correlated with a country or territory's annual commercial services exports and imports.

Over the past seven months, I have compiled, read, and analyzed data privacy laws and bills from 202 countries or territories. Of these 202 countries or territories, approximately 50 percent have enacted national data privacy frameworks—and for some, the levels of privacy protections and penalties vary widely.^a For example, approximately 37 percent of entities have enacted omnibus national privacy laws that broadly apply to all sectors, regions, and types of data (e.g., Argentina, France), while approximately 13 percent have sectoral laws that only cover specific industries, regions, or types of data (e.g., United States, Bolivia). Similarly, approximately 37 percent of entities have national privacy laws that limit data transfers to third-party countries that do not meet an “adequate” level of privacy protection (e.g., Germany, Japan), while around 63 percent either do not have national privacy laws or have laws without “data adequacy” requirements (e.g., United States, Bhutan). Finally, governments have widely-differing maximum levels of financial penalties for businesses that violate privacy laws, ranging from

^a In my study, I only assess national privacy laws passed on or before December 31, 2018. Therefore, any laws passed on or after January 1, 2019 are excluded from this calculation.

approximately \$259 in Nepal's Privacy Act to approximately \$22 million (or, if greater, four percent of a company's global annual revenue) in the European Union's General Data Protection Regulation (GDPR).^b

As I discuss in Section II, the passage of the GDPR has prompted increased scholarly discourse about the effects of data privacy laws. Governments have enacted dozens of data privacy laws and regulations between 2005 and 2018, with the GDPR as one prominent example. The EU adopted the GDPR in April 2016, and when it came into effect in May 2018, it replaced the European Data Protection Directive of 1995 and imposed new privacy obligations and higher non-compliance penalties on almost all businesses that collect, process, or store data from EU residents (including businesses not based in Europe).

Meanwhile, the United States has not yet enacted a comprehensive federal privacy law (Chin, 2018). Instead, it has dozens of sectoral federal or state laws that regulate some aspect of privacy, including the Privacy Act of 1974, Children's Online Privacy Protection Act of 1998, and California Consumer Privacy Act of 2018 (CCPA), among others. However, multiple members of Congress have introduced federal baseline privacy legislation over the past two years, and current and future research on the relationship between privacy laws and international trade can have significant policy implications in the legislative process.

I organize this thesis as follows: in Section II, I discuss recent academic literature related to privacy laws and international trade; in Sections III and IV, I outline my theoretical and empirical models of analysis, where I employ linear and fixed-effects regression models to evaluate the relationship between national data privacy laws and annual commercial services

^b In this paper, all monetary values are listed in USD with a conversion rate as of December 31, 2019.

exports and imports. In Section V, I explain my data; in Section VI, I present my results. Finally, in Section VII, I report my findings and discuss the public policy implications of my study, as well as the limitations and opportunities for further research.

II. LITERATURE REVIEW

In recent years, the internet has facilitated the cross-border transfer of commercial goods and services. According to Meltzer, this development has positive implications for commerce: “traditional manufacturing and services companies [benefit] from internet-enabled applications and commerce. For instance, the internet has enabled entrepreneurs and businesses to access services and customers globally at lower costs” (Meltzer, 2014).

However, with the rise of the internet comes the challenge of data protection (Carlin, 1998). In a recent United Nations Conference on Trade and Development (UNCTAD) report, Fredriksson et al. writes that “data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result” (Fredriksson et al., 2016). Fredriksson et al. thus suggests that the stringency of data protection regulations can negatively impact international trade, while others, such as Kerry, argue that national privacy laws are “essential to competing in a global digital economy” (Kerry, Forthcoming).

In both scenarios, it becomes clear that research related to data protection and international trade is increasingly relevant in the global economy. According to Tesfachew, “understanding different approaches and potential avenues for establishing more compatible legal frameworks at national, regional, and multilateral levels is important for facilitating international trade and online commerce” (Fredriksson et al., 2016). Next, I discuss both of these countervailing points of view regarding the effects of data privacy laws on international trade.

A. COMPLIANCE COSTS

Because new regulations can induce high compliance costs for businesses, many industry groups have historically argued that certain privacy laws can have negative economic effects. For example, Gary Schapiro, president of the Consumer Technology Association, testified in April 2018 before a House Oversight subcommittee that the GDPR was “going to hurt American companies” and that it indirectly was “also going to kill people” (Schapiro, 2018). In context, the IAPP and Ernst and Young estimate that the GDPR could cost companies an estimated \$8 billion in legal and compliance costs (Carson, 2018). Berkeley Economic Advising and Research estimate that the CCPA could cost companies up to \$55 billion in initial compliance expenses (Roland-Holst, et al., 2019).

Academic scholars have also warned that laws like the GDPR could have potential unintended consequences. According to Mattoo and Meltzer, one of the GDPR’s largest challenges is to support digital trade while simultaneously maintaining privacy protections. They explain that such regulations—that both induce high administrative costs and broadly apply to most companies—could especially harm developing countries and small businesses (Mattoo & Meltzer, 2018). Similarly, Shaffer writes that governments must weigh both privacy protections and compliance costs when considering privacy regulations: “the concept of ‘fundamental rights,’ however, is problematic when advocates give ‘rights’ an infinite value, eliminating the possibility of any cost-benefit analysis involving competing values ... Efficiency is reduced because privacy interests are not balanced against other societal concerns, including access to low-cost goods” (Shaffer, 2000).

B. INTEROPERABILITY OF NATIONAL PRIVACY LAWS

According to Swire, privacy regulations could harm international trade not only through higher compliance costs, but additionally through questions of international jurisdiction. In cases of cross-border data transfers, Swire says that this jurisdictional uncertainty could present businesses with compliance issues. However, he posits that the harmonization, or “approximation,” of laws between countries is one way to prevent international conflicts (Swire, 1998). Even if countries have different data privacy legal frameworks, the interoperability of frameworks can help businesses offer products and services more consistently between countries (Kerry, 2016).

Furthermore, other scholars suggest that uncertainty around new regulations, such as the GDPR, could cause a downward pressure on investment. Tesfachew writes: “in [some] cases, the various pieces of legislation introduced are incompatible with each other. ... Such lack of clarity creates uncertainty for consumers and businesses, limits the scope for cross-border exchange, and stifles growth” (Fredriksson et al., 2016). Tesfachew summarizes a concern that the legal uncertainty surrounding conflicting country-specific laws could negatively impact investment and emerging technologies.

C. DATA ADEQUACY REQUIREMENTS

In June 1977, Senator George McGovern, who served on the Senate Committee on Foreign Relations, wrote in *The New York Times* that “one way to ‘attack’ a nation such as the United States which depends heavily on information and communications is to restrain the flow of information.” Since then, several governments, such as the EU and India, have adopted privacy laws that restrict information flows under certain conditions. Under Article 45 of the GDPR, for

example, businesses may only transfer data from the European Union to non-EU countries if the European Commission determines that the receiving country meets “adequate” privacy standards (Mulligan et al., 2019). Mattoo and Meltzer write that the GDPR’s data adequacy provisions are “likely to affect trade that depends on data flows” (Mattoo & Meltzer, 2018).

Data adequacy requirements (i.e., requiring certain privacy standards for cross-border data transfers) are distinct from data localization laws (i.e., requiring a company to store data on a domestic server), although both can present digital trade barriers for companies. Countries might restrict cross-border data flows for multiple reasons, including privacy, cybersecurity, economic protectionism, or political censorship (Fefer, 2019). Meltzer argues that governments can use data localization rules to promote domestic businesses at the expense of foreign ones; furthermore, some governments such as China and Iran have even used data flow restrictions to block access to online political commentary (Meltzer, 2014).

Many U.S. trading partners, such as Argentina, Israel, and Japan, currently meet Europe’s data adequacy requirements—but the United States does not. In the absence of a legal framework that meets data adequacy provisions, countries such as the United States can reach accommodations allowing businesses to demonstrate privacy commitments through signed legal contracts or other industry-wide standards. However, legal challenges to such accommodations, like the EU-U.S. Privacy Shield, result in regulatory uncertainty that could also affect businesses operating internationally (Raul et al., 2015). Eger recommends that the United States pass a federal privacy law to help trade: “both the informational and economic functions of transnational communication are threatened, however, by the ever-increasing restrictions growing out of foreign privacy and data protection laws. ... the United States must develop a

unified national policy respecting transnational data flows” (Eger, 1978). Eger goes further to suggest that any restrictions on the free flow of data, such as data adequacy requirements, could act in function like a non-tariff trade barrier. In other words, restricting cross-border data flows could hurt countries, and especially exports for developing countries (Meltzer, 2014).

D. CONSUMER TRUST IN COMPANIES

Despite these challenges, a number of scholars and privacy advocates suggest that privacy regulations could boost international trade. For example, national privacy frameworks could improve consumer confidence in information privacy and provide some degree of long-term regulatory certainty for companies. In 2015, after the Snowden leaks, the Pew Research Center surveyed approximately 600 Americans and found that 33 percent reported that they were “not at all confident” that companies or retailers would keep their data private and secure—and only four percent were “very confident” (Madden & Rainie, 2015). Tesfachew writes that “creating trust online is a fundamental challenge to ensure that opportunities emerging in the information economy can be fully leveraged” (Fredriksson et al., 2016).

However, not all scholars agree on the effects of privacy and consumer trust on international trade. In fact, one recent study suggests that there is no change in consumer behavior due to privacy incident notifications. In 2009, Muntermann and Roßnagel compared stock market reactions following privacy incident notifications and found that, for companies, the financial effects of privacy incidents were minimal compared to disclosures of other types of negative events. Therefore, the two researchers concluded that privacy incident notifications do not generally affect macroeconomic markets (Muntermann & Roßnagel, 2009).

E. DIPLOMACY AND PRIVACY VALUES

Finally, some researchers describe the possibility for a country to demonstrate diplomatic good will (or “soft power”) through its data privacy regime. Kerry posits that liberal democracies can align themselves with their geopolitical or economic allies by passing meaningful privacy legislation. He writes that the international community has doubted U.S. privacy values due to recent attention to Facebook and Snowden, and that these events have highlighted the breadth of data collection and lack of U.S. regulation (Kerry, Forthcoming).

Kerry suggests that a U.S. federal privacy law would better align the United States with its international allies, while other scholars contend that there are broader cultural differences in privacy. To Whitman, “it often seems obvious [to Europeans] that Americans do not understand the imperative demands of privacy at all,” explaining that Americans are more likely than Europeans to discuss their salaries or share their credit scores (Whitman, 2004). To Sedgewick, “points of international agreement, particularly shared norms and concerns between the United States and Europe, can be useful in bridging the differences between their existing digital privacy frameworks. However, distrust and fear of the others’ approach have created an environment hostile to reconciliation of the two regimes” (Sedgewick, 2017). In some cases, governments can influence each other: referring to the “theme of foreign market power,” Shaffer explains that market power drives international data privacy negotiations over both social regulation and trade (Shaffer, 2000).

F. CONTINUING THE DISCUSSION

Many of these issues are largely legal or theoretical—because many countries have enacted privacy laws within the past couple decades, not much quantitative data have yet become

available to explain any correlation between national privacy laws and international trade.

Therefore, this thesis is a preliminary endeavor to quantify such a relationship. By comparing countries and territories' annual commercial services exports and imports with their national privacy frameworks from 2005 to 2018, I consider the issues raised by Meltzer, Mattoo, Kerry, Eger, and others.

Furthermore, I build upon recent literature by analyzing several major factors raised (e.g., the enactment of a national privacy law; the enactment of an omnibus national privacy law covering all sectors, the enactment of data adequacy requirements; and the strictness of a national law as measured by monetary penalties). In doing so, I seek to motivate further research and analysis into the relationship between national privacy frameworks and international trade.

III. THEORETICAL MODEL

Based on recent literature, I hypothesize that the enactment of a national privacy law has a positive correlation with a country or territory's international trade prospects. To explore the relationship between national privacy laws and trade, I develop the following general formula:

$$\text{International Trade} = f(\text{Privacy Law}, \text{GDP}, \text{Population}, \text{Technology Adoption}, e) \quad (1)$$

With this theoretical model, my primary objective is to measure the magnitude of the *Privacy Law* variable, which represents the status of a country or territory's national privacy framework in a given year. In addition to the *Privacy Law* variable, I control for several other factors that could also impact a nation's international trade prospects. These include *GDP*, *Population*, and *Technology Adoption*, all of which are positively correlated with both *Privacy Law* and *International Trade*. Finally, "e" represents random error. Using this general formula, I predict each country or territory's annual trade statistics given its national privacy framework and control variables.

In Section IV, I explain the empirical model that I use to test this theoretical model, and in Section V, I discuss my data in greater detail.

IV. EMPIRICAL MODEL

To explore the relationship between national privacy laws and international trade, I use linear regression and fixed-effects models for each of the following eight formulas:

$$\text{Annual Commercial Services Exports} = \beta_0 + \beta_1(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (2)$$

$$\text{Annual Commercial Services Exports} = \beta_0 + \beta_2(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (3)$$

$$\text{Annual Commercial Services Exports} = \beta_0 + \beta_3(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (4)$$

$$\text{Annual Commercial Services Imports} = \beta_0 + \beta_1(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (5)$$

$$\text{Annual Commercial Services Imports} = \beta_0 + \beta_2(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (6)$$

$$\text{Annual Commercial Services Imports} = \beta_0 + \beta_3(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (7)$$

$$\text{Annual Commercial Services Exports} = \beta_0 + \beta_4(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (8)$$

$$\text{Annual Commercial Services Imports} = \beta_0 + \beta_4(\text{Privacy Law}) + \beta_5(\text{GDP}) + \beta_6(\text{Population}) + \beta_7(\text{Mobile Subscriptions}) + \varepsilon \quad (9)$$

In these regression models, I use four separate independent variables to measure national privacy frameworks in each country or territory (β_1 , β_2 , β_3 , and β_4). The first three variables are binary. β_1 , β_2 , and β_3 each represent “yes” or “no” responses whether each entity meets the following standards in a given year: has enacted a national privacy law (β_1), has enacted an omnibus national privacy law covering all data, sectors, and regions (β_2), and has enacted a national privacy law with data adequacy provisions (β_3). In models (8) and (9), the maximum monetary penalty (β_4) is a continuous variable representing the maximum monetary penalty per privacy violation; countries or territories without any national privacy laws receive a “0” in this

coding. Countries or territories with multiple sectoral national privacy laws are omitted from models (8) and (9) due to the possibility of many values for monetary penalties. For example, the United States, with numerous sectoral federal and state laws, would receive a “1” for β_1 , a “0” for β_2 , a “0” for β_3 , and would be excluded from the coding of β_4 .

Linear regression models, or ordinary least squares (OLS) regression models, predict the value of the dependent variable based on the input independent variables in the model. However, the possibility of omitted variable bias exists if I exclude independent control variables from the model that are correlated with both *Privacy Law* and *Annual Commercial Services Exports* or *Imports*. For this reason, I also use fixed-effects regression models to control for demographic factors that either do not change over time or change at a constant rate over time. For both types of regression models, I additionally control for known confounding variables: GDP (β_5), population size (β_6), and technology adoption (β_7 , as measured by number of mobile subscriptions per 100 people).

I predict that each of these three demographic variables (β_5 , β_6 , and β_7) have a positive correlation with a country or territory’s level of international trade; if uncontrolled for in the model, omitted variable bias could occur. In addition, as I hypothesize that national privacy laws ultimately benefit international trade, I predict that the four independent variables representing national privacy laws (β_1 , β_2 , β_3 , β_4) will have a positive correlation with the dependent variable, commercial services exports and imports.

In the next section, I discuss the data that I use to estimate this empirical model, including how I code the “Privacy Law” independent variables and choose the control and dependent variables.

V. DATA

A. INDEPENDENT VARIABLE: PRIVACY LAWS

To catalogue the privacy legal frameworks of these 202 countries and territories, I first access the original language of all publicly-accessible national privacy laws to the extent possible, using online translators if necessary. Although many laws are available on government websites, I find that some laws are not easily translatable or machine-readable, and in some cases, not available online at all. For this reason, I also use dozens of legal resources and media reports to both supplement and fact-check my research. These include analyses from Bloomberg Law, DLA Piper, Lexology, UNCTAD, Baker McKenzie, Graham Greenleaf, Commission Nationale de l'Informatique et des Libertés (CNIL), among others (see Appendix A). The independent variable *Privacy Law* represents the culmination of this comprehensive analysis of national data privacy laws.

After compiling a comprehensive database of national privacy laws, I then create three binary variables as described in Section IV: β1) Has the country or territory enacted a national privacy law, either sectoral or omnibus? β2) Has the country or territory enacted an omnibus national privacy law covering all types of data, regions, and sectors? β3) Has the country or territory enacted a national privacy law with data adequacy requirements? Each of these three variables is coded “1” for “yes” or “0” for “no,” corresponding with each entity’s status every year. In addition, I code a fourth variable, β4, a continuous variable that represents the maximum financial penalty per privacy law violation (in USD; adjusted for inflation). I report the status of each of these four variables for every year between 2005 and 2018.

It is important to note the limitations of the *Privacy Law* independent variable. β_1 , β_2 , and β_3 only code the enactment of laws—they do not account for the enforcement of laws, nor do they incorporate trade accommodations like the EU-U.S. Privacy Shield. β_2 is relatively straightforward—does the entity have a comprehensive national privacy framework or not—but β_1 requires judgment calls as to what qualifies as a data privacy law (for example, I counted sectoral telecommunications privacy laws, but did not include general constitutional principles or freedom of information laws). Furthermore, β_4 only considers financial penalties, and does not factor criminal or non-financial penalties into the analysis. Finally, as mentioned earlier, I omitted countries or territories with multiple sectoral national privacy laws from the coding of β_4 due to the possibility of numerous values of monetary penalties. Because β_4 only includes countries or territories with omnibus national privacy laws and those with none, the sample size for this variable is smaller than β_1 , β_2 , and β_3 (see Table 1). In summary, this coding is a preliminary endeavor and does not fully capture the complexity of modern data privacy legal frameworks.

B. DEPENDENT VARIABLE: INTERNATIONAL TRADE

To measure my dependent variable, international trade, I turn to the World Trade Organization's (WTO) public database of international trade statistics by nation and year. From this database, I create a continuous variable that reports each country or territory's total annual commercial services exports and imports from 2005 to 2018—this includes finance, internet, technology, tourism, hospitality, and other services.^c

^c World Trade Organization (2005 to 2018). Trade in commercial services. Available from World Trade Organization: <https://timeseries.wto.org/>

In addition to commercial services, the WTO also collects data regarding annual commercial merchandise exports and imports from 2005 to 2018, and the World Bank makes data available on high technology exports by nation from 2007 to 2018.^d In an ideal study, I would be able to collect the precise breakdown of commercial services and merchandise exports and imports by industry and sector, as privacy laws can affect different businesses in different ways. However, in this study, I am only able to use general, publicly-available trade statistics.

Due to this limitation, I choose to measure international trade using commercial services exports and imports, rather than merchandise exports and imports. When it comes to merchandise, there is a wide range of exports and imports by country; for example, Germany's leading exports are machinery and vehicles, which may depend less on customer personal information than ICT goods do (CIA World Factbook). Although privacy laws also affect services differently by sector, the overall trade number is still relevant because almost any company providing internet-based services across borders will need to consider data protection.

Finally, I elect not to use the World Bank's data on high technology exports due to the scope of missing information—the World Bank has data available on approximately 123 countries, which would reduce my sample size from roughly 2,600 to 1,474.

C. CONTROL VARIABLES

Lastly, I utilize three control variables in my regression model: GDP, population size, and technology adoption (as measured by the number of mobile subscriptions per 100 people).^e

^d World Trade Organization (2005 to 2018). Merchandise trade values. Available from World Trade Organization: <https://timeseries.wto.org/>

World Bank (2007 to 2018). High-technology exports (current US\$). Available from World Bank: <https://data.worldbank.org/indicator/TX.VAL.TECH.CD>

^e World Bank (2005 to 2018). GDP (current US\$). Available from World Bank: <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD>

Some additional factors that could potentially contribute to omitted variable bias are education, workforce size, and urbanization, as all three are indicators of economic development. The omission of an education control variable in this study is also a result of a lack of publicly-available data. Although the World Bank has data on primary, secondary, and tertiary school enrollment, information from approximately one-third of listed countries are missing.^f When including the World Bank school enrollment data, the number of observations in the sample decreases from approximately 2,400 to 1,500 observations and the education variable itself is statistically insignificant across most of the regression models. The World Bank also has publicly-available data on labor force size and urban population from 2005 to 2018, but in addition to missing countries, I encounter a high level of multicollinearity between the labor force, total population, and urban population variables, resulting in statistically insignificant coefficients for one or all three variables when included together in the same regression (See Appendix B).^g Therefore, I choose to omit education, workforce size, and urbanization from the regressions in Tables 1, 2, and 3.

In Tables 1, 2, and 3, I use the World Bank's public data on the number of mobile cellular subscriptions per 100 people from 2005 to 2018 as the best available measure of technology

World Bank (2005 to 2018). Population, total. Available from World Bank:

<https://data.worldbank.org/indicator/sp.pop.totl>

^f World Bank (2005 to 2018). School enrollment, primary (% gross). Available from World Bank:

<https://data.worldbank.org/indicator/SE.PRM.ENRR?view=chart>

World Bank (2005 to 2018). School enrollment, secondary (% gross). Available from World Bank:

<https://data.worldbank.org/indicator/SE.SEC.ENRR?view=chart>

World Bank (2005 to 2018). School enrollment, tertiary (% gross). Available from World Bank:

<https://data.worldbank.org/indicator/SE.TER.ENRR?view=chart>

^g World Bank (2005 to 2018). Labor force, total. Available from World Bank:

<https://data.worldbank.org/indicator/SP.URB.TOTL>

World Bank (2005 to 2018). Urban population. Available from World Bank:

<https://data.worldbank.org/indicator/SP.URB.TOTL>

adoption.^h To control for technology adoption, I also experiment with substituting access to electricity, but I find that access to electricity is generally insignificant in the fixed-effects model, possibly due to a lack of year-to-year variation from 2005 to 2018 (many countries remain constant during this period at 100 percent), as well as missing data for some countries (See Appendix B).ⁱ Therefore, the regressions in Tables 1, 2, and 3 use the number of mobile subscriptions as a statistically significant—although not perfect—indicator of technology adoption from 2005 to 2018.

For ease of interpretation, I transform all continuous variables in the model to log variables. This allows me to estimate the elasticity of the dependent variable: how either a percentage change (for β_4 , β_5 , β_6 , or β_7) or a binary change (for β_1 , β_2 , β_3) in x affects a percentage change in y . The following table summarizes descriptive statistics for my independent and dependent variables.

^h World Bank (2005 to 2018). Mobile cellular subscriptions (per 100 people). Available from World Bank: <https://data.worldbank.org/indicator/it.cel.sets.p2>

ⁱ World Bank (2005 to 2018). Access to electricity (% of population). Available from World Bank: <https://data.worldbank.org/indicator/eg.elc.accs.zs>

TABLE 1: DESCRIPTIVE STATISTICS

Variable	N	Mean	Std. Dev.	Minimum	Maximum
<i>Law*</i>	2632	0.514	0.499	0	1
<i>Law – All Sectors*</i>	2605	0.375	0.484	0	1
<i>Law – Data Adequacy*</i>	2479	0.372	0.483	0	1
<i>Monetary Penalty (Log)</i>	679	10.637	3.535	0	16.924
<i>Services Exports (Log)</i>	2557	21.672	2.345	14.509	27.443
<i>Services Imports (Log)</i>	2544	21.876	2.141	16.899	30.651
<i>GDP (Log)</i>	2568	24.185	2.344	16.899	30.651
<i>Population (Log)</i>	2632	15.594	2.104	9.21	21.055
<i>Mobile Subscriptions (Log)</i>	2560	4.269	0.857	-1.336	5.844
<i>Secondary Education (Log)</i>	1779	4.321	0.467	1.78	5.099
<i>Labor Force (Log)</i>	2464	15.057	1.809	10.484	20.484
<i>Urban Population (Log)</i>	2604	14.975	2.126	8.511	20.529
<i>Electricity Access (Log)</i>	2398	4.228	0.665	0.405	4.605

*Indicates a binary variable, where “1” indicates the presence of a condition and “0” indicates the absence of a condition.

VI. RESULTS

After compiling this dataset, I use my empirical model to test the relationship between national privacy laws and international trade. First, I use a linear regression to compare four measures of privacy frameworks (enactment of a national privacy law, enactment of a national privacy law applying to all sectors, enactment of a national privacy law with data adequacy requirements, and maximum monetary penalties) with the annual commercial services exports and imports of each country or territory. Second, I use a fixed-effects model to compare these same variables but additionally controlling for unknown or unobserved variables that either do not change over time or change at a constant rate over time. When comparing these two models, I have found positive and statistically significant correlations between national privacy laws and commercial services exports and imports—consistent with my hypothesis—although the magnitude of the correlation and the level of statistical significance varies with each of the two types of regressions.

TABLE 2: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF NATIONAL PRIVACY LAWS AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES EXPORTS (2005-2018)

VARIABLES	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects	(5) OLS	(6) Fixed Effects
<i>Law – Enacted</i>	0.371*** (0.0456)	0.0979* (0.0499)				
<i>Law – All Sectors</i>			0.493*** (0.0416)	0.0999** (0.0478)		
<i>Law – Data Adequacy</i>					0.491*** (0.0418)	0.127*** (0.0477)
<i>GDP (Log)</i>	1.092*** (0.0170)	0.639*** (0.0809)	1.070*** (0.0168)	0.626*** (0.0783)	1.056*** (0.0165)	0.625*** (0.0788)
<i>Population (Log)</i>	-0.363*** (0.0184)	0.576* (0.294)	-0.331*** (0.0186)	0.562* (0.289)	-0.315*** (0.0186)	0.516* (0.300)
<i>Mobile Subscriptions (Log)</i>	0.105*** (0.0312)	0.0899* (0.0521)	0.116*** (0.0311)	0.0993* (0.0556)	0.140*** (0.0325)	0.113** (0.0564)
<i>Constant</i>	0.272 (0.180)	-3.245 (4.464)	0.255 (0.177)	-2.768 (4.351)	0.286 (0.177)	-2.052 (4.505)
<i>Observations</i>	2,461	2,461	2,434	2,434	2,313	2,313
<i>R-squared</i>	0.863	0.487	0.863	0.486	0.860	0.493
<i>F test</i>	5460***	89.17***	5620***	92.88***	5314***	93.61***
<i>Number of countries</i>		185		183		174

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

The findings in Table 2 generally suggest that—holding all variables in the models constant—a positive correlation exists between national privacy laws and commercial services exports. However, there is a quantitative difference between the magnitude and statistical significance of the privacy law independent variables in the OLS and fixed-effects models.

Columns 1, 3, and 5 display the results of the three linear regressions. Using an OLS model, I find that countries or territories that have enacted any national privacy law (including sectoral laws, omnibus laws, and laws with data adequacy provisions) have higher commercial services exports than those that have not enacted any national privacy law, holding constant the country

or territory's GDP, population size, and number of mobile subscriptions. For example, the OLS model indicates that, on average, countries or territories that have enacted at least one national privacy law generate 44.9 percent higher annual commercial services exports than those that have not, holding constant GDP, population size, and technology adoption. The magnitude of the correlation increases with the comprehensiveness of the legislation—on average, countries or territories that enact a national privacy law applying to all sectors generate 63.7 percent higher annual commercial services exports than those that have not enacted any national privacy laws, holding all variables in the model constant. In all three linear regressions (Columns 1, 3, and 5), the results are statistically significant at a 99 percent confidence level. The R-squared of the OLS models (Columns 1, 3, and 5) are around 0.86, indicating that the independent variables in the regression—privacy legal framework, GDP, population size, and mobile subscriptions—predict approximately 86 percent of the variance in the dependent variable, commercial services exports.

Although the OLS regressions in Columns 1, 3, and 5 support my hypothesis, the possibility of omitted variable bias exists within these results. Omitted variable bias—which occurs as a result of non-random omission of variables that are correlated with both the independent and dependent variables in a regression—could exist in the linear regression models because I only control for variables with publicly-accessible data. In other words, I currently control for GDP, population size, and technology adoption—but if other variables exist that correlate with both national privacy laws and commercial services exports, then omitted variable bias may exist in these OLS models.

To help solve the problem of omitted variable bias, I next use a fixed-effects model. Fixed-effects models control for unobserved variables that are either held constant over time or change

at a constant rate over time. In this model, it is possible that fixed-effects may control for unobservable country-level variables such as time-invariant trade partnerships or cultural attitudes toward privacy. In addition, I continue to include known control variables that vary over time: GDP, population size, and technology adoption.

After controlling for time-invariant variables, the fixed-effects models (in Columns 2, 4, and 6) still indicate a positive and statistically significant relationship between national privacy laws and commercial services exports. However, the magnitude and statistical significance of the privacy law coefficients change. In Column 4, countries or territories that have enacted at least one national privacy law governing all sectors generate, on average, 10.5 percent higher commercial services exports than those that have not enacted any privacy laws, holding all variables in the model constant. This result is statistically significant at a 5 percent confidence level, with R-squared at approximately 0.486. Although the results in Columns 2, 4, and 6 still indicate a positive correlation between national privacy laws and commercial services exports, the different in magnitude between the parallel OLS regressions indicate that at least part of the results observed in Columns 1, 3, and 5 may encompass omitted variable bias. The fixed-effects models control for time-invariant variables, but none of the models control for unobserved confounding variables that vary with time.

TABLE 3: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF NATIONAL PRIVACY LAWS AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES IMPORTS (2005-2018)

VARIABLES	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects	(5) OLS	(6) Fixed Effects
<i>Law – Enacted</i>	0.091*** (0.0271)	0.133** (0.0556)				
<i>Law – All Sectors</i>			0.190*** (0.0251)	0.111** (0.0650)		
<i>Law – Data Adequacy</i>					0.207*** (0.0257)	0.113 (0.0690)
<i>GDP (Log)</i>	1.011*** (0.0114)	0.792*** (0.0814)	0.995*** (0.0108)	0.791*** (0.0822)	0.991*** (0.0110)	0.787*** (0.0849)
<i>Population (Log)</i>	-0.21*** (0.0119)	0.467** (0.204)	-0.20*** (0.0114)	0.490** (0.202)	-0.20*** (0.0116)	0.481** (0.210)
<i>Mobile Subscriptions (Log)</i>	-0.00741 (0.0206)	0.0116 (0.0322)	-0.00818 (0.0206)	0.0201 (0.0346)	-0.00960 (0.0214)	0.0242 (0.0356)
<i>Constant</i>	0.702*** (0.124)	-4.763 (3.204)	0.825*** (0.119)	-5.106 (3.143)	0.929*** (0.121)	-4.903 (3.261)
<i>Observations</i>	2,448	2,448	2,421	2,421	2,300	2,300
<i>R-squared</i>	0.929	0.601	0.928	0.597	0.928	0.589
<i>F test</i>	10421***	102.1***	10235***	89.45***	9742***	78.37***
<i>Number of countries</i>		184		182		173

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Like the results in Table 2, I generally find a positive and statistically significant correlation between national privacy laws and commercial services imports in Table 3. The results of the OLS regressions are displayed in Columns 1, 3, and 5, while the results of the fixed-effects models are displayed in Columns 2, 4, and 6.

Interestingly, the results of the OLS and fixed-effects regressions are more similar when measuring commercial services imports, as opposed to commercial services exports. For example, on average, countries or territories that enact at least one national privacy law generate 9.5 percent higher annual commercial services imports as calculated by an OLS regression

(Column 3) and 14.2 percent higher annual commercial services imports as calculated by a fixed-effects regression (Column 4) than those that have not, holding all variables in the model constant. Furthermore, countries or territories that enact at least one national privacy law applying to all sectors generate 20.9 percent higher annual commercial services imports as calculated by an OLS regression (Column 1) and 11.7 percent higher annual commercial services imports as calculated by a fixed-effects regression (Column 2) than those that have not enacted any national privacy legislation, holding all variables in the model constant. Additionally, R-squared is higher for commercial services imports than exports, equating to over 0.92 for the linear regressions (Columns 1, 3, 5) and about 0.59 to 0.60 for the fixed-effects models (Columns 2, 4, 6).

The smaller difference in magnitude of the privacy coefficients between the OLS and fixed-effects models may suggest that the effects of omitted variable bias in the linear regressions (Columns 1, 3, and 5) are lower for commercial services imports than exports. However, it is important to note that the magnitude of the correlation is also comparatively lower for commercial services imports, and the coefficient for enacted privacy laws with data adequacy provisions has a P-value of 0.16, which is above a 10 percent level of statistical significance. However, the OLS and fixed-effects regression results for enacted privacy laws and enacted omnibus privacy laws are both statistically significant at a 95 percent confidence level, with P-values ranging from 0.024 to less than 0.000. Furthermore, it is also important to note that (as with Table 2), the fixed-effects models in Table 3 only control for time-invariant variables, and do not control for unobserved confounding variables that change over time.

TABLE 4: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF MAXIMUM MONETARY PENALTIES AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES EXPORTS AND IMPORTS (2005-2018)

VARIABLES	<i>Exports</i>		<i>Imports</i>	
	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects
<i>Maximum Monetary Fine (Log)</i>	0.0241*** (0.0066)	0.0369*** (0.005)	0.0152*** (0.0054)	0.031*** (0.0044)
<i>GDP (Log)</i>	1.1809*** (0.0304)	0.6452*** (0.0957)	1.0991*** (0.0238)	0.9244*** (0.0783)
<i>Population (Log)</i>	-0.5248*** (0.0335)	0.9969** (0.142)	-0.3401*** (0.0267)	0.7887** (0.1628)
<i>Mobile Subscriptions (Log)</i>	0.3348*** (0.0897)	0.258** (0.1148)	0.0759 (0.0545)	0.052 (0.0669)
<i>Constant</i>	-0.3851 (0.3905)	-10.81*** (1.944)	0.0379 (0.2652)	-13.521*** (1.9684)
<i>Observations</i>	1,642	1,642	1,642	1,642
<i>R-squared</i>	0.872	0.533	0.925	0.744
<i>F test</i>	3303***	53.12***	5778***	60.10***
<i>Number of countries</i>		142		142

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Finally, Table 4 shows the OLS and fixed-effects regression results of maximum monetary penalties for privacy law violations and commercial services exports and imports. As with Tables 2 and 3, I generally find positive and statistically significant correlations between privacy laws and commercial services exports and imports in Table 4. In Table 4, I now compare each entity's commercial services exports and imports with the maximum monetary penalty in enacted privacy laws, holding constant GDP, population size, and number of mobile subscriptions. Here, the results of the OLS and fixed-effects regressions are even more similar than in Table 3: in Table 4, each one percent increase in maximum monetary penalty is correlated with a 2.41 percent increase in annual commercial services exports and a 1.52 percent increase in commercial

services imports as measured by an OLS regression (Columns 1 and 3), and a 3.69 percent increase in annual commercial services exports and 3.1 percent increase in commercial services imports, as measured by a fixed-effects model (Columns 2 and 4), holding all variables in the model constant. Each of these results is statistically significant at a 99 percent confidence level.

Building on my discussion of data limitations in Section V, these findings are limited by several factors: data access, the inability to code the complexities of privacy legislation into my independent variable, and the variation in commercial activity per country or territory. Although the R-squared and P-value of these regression models are generally promising—as they show that the independent variables included in the models predict a significant percentage of the variation in the dependent variable, and there is a low probability that I find these results by chance—it is important to note that, due to the limitations of my study, I am unable to infer causation from any of these observed correlations.

VII. CONCLUSION AND POLICY RECOMMENDATIONS

With the above linear and fixed-effects regression models, I find that the enactment of comprehensive national privacy laws has a positive and statistically significant correlation with a country or territory's annual commercial services exports and imports. Although I acknowledge the limited nature of my study, my results lend preliminary support to Kerry, Meltzer, Mattoo, Tesfachew, and other scholars who argue that national privacy laws can positively affect international trade.

Based on these results, as well as recent literature, I support the consideration of international trade implications as Congress continues to develop federal privacy legislation. This consideration is already present among federal agencies, stakeholders, and Congress itself. The National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce requested comments on a federal privacy framework in 2018, which, among other provisions, included a "regulatory landscape that is consistent with the international norms and frameworks in which the United States participates" (NTIA, 2018). In their reply comments, several organizations including Google and Verizon emphasized a need to unify U.S. privacy policy with international standards.

Furthermore, Senate and House committees have held multiple hearings on the GDPR and other international privacy standards, including a Senate Commerce Committee hearing on May 1, 2019, where Ranking Member Maria Cantwell (D-WA) stated: "we also need to work with our international partners to form coalitions around cybersecurity standards and work towards harmonizing privacy and cybersecurity regulations" (Cantwell, 2019).

My research, in conclusion, supports the academic theory that privacy regulations have a direct relationship with trade, as well as the related policy argument that a comprehensive U.S. federal privacy law would help U.S. trade. In turn, I recommend that Congress continue to develop privacy legislation—and continue to seek advice from U.S. trade allies—in order to promote trade certainty for U.S. businesses and individuals. As I describe earlier, my research only measures basic measures of national privacy frameworks, as well as overall levels of commercial services exports and imports. It is one way to approach an inquiry—but it does not give us the complete picture, as systems of privacy laws and international trade are both extremely complex.

But where I leave off, there are infinite opportunities for future research. It would be especially interesting to see research into the nuances of privacy law—for example, how national privacy laws are enforced and penalties given, and the related impacts on diverse industries and sectors. In addition, there are political and economic interests into researching individual countries: for example, how major trade partners like the United States, European Union, and China are uniquely affected by changes in privacy legal frameworks in recent years. Furthermore, future research that finds a way to capture some of the other confounding variables that are correlated with international trade—perhaps either through proxy variables or the accumulation of additional data over time—could bring us closer to quantifying a relationship between national privacy laws and international trade. Given a growing political and economic interest for federal privacy legislation in the United States, now is an important time to build on the academic research in this field.

APPENDIX A: INTERNATIONAL PRIVACY LEGAL RESOURCES

Al-Fawzan, N., & Elsayed, O. Data protection in the Kingdom of Saudi Arabia: A primer. Latham & Watkins LLP. <https://www.lw.com/presentations/Data-Protection-in-the-Kingdom-of-Saudi-Arabia>

Anderson, C., & Brewitt, B. (2019, September 3). New Cayman Islands data protection law, 2017 coming into effect. Foley Hoag LLP. <https://www.jdsupra.com/legalnews/new-cayman-islands-data-protection-law-11478/>

(2011, September 19). Angola passes personal data protection law. Privacy & Information Security Law Blog. *Hunton Andrews Kurth*. <https://www.huntonprivacyblog.com/2011/09/19/angola-passes-personal-data-protection-law/>

(2018, April 18). Beyond the GDPR: What you should know about Japan's Act on the Protection of Personal Information. Focal Point Insights. <https://blog.focal-point.com/beyond-the-gdpr-what-you-should-know-about-japans-act-on-the-protection-of-personal-information>

Bowman, C. M., & Reardon, J. (2016, November 4). Privacy law in Saudi Arabia: A primer for businesses. Corporate Counsel. <https://privacylaw.proskauer.com/files/2016/11/Privacy-Law-in-Saudi-Arabia.pdf>

(2017) Building trust across cultures: Privacy and data protection. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-building-trust-across-cultures.pdf>

(2019, September 9). Cayman Islands data protection law goes into force this month. Privacy & Information Security Law Blog. *Hunton Andrews Kurth*. <https://www.huntonprivacyblog.com/2019/09/09/cayman-islands-data-protection-law-goes-into-force-this-month/>

Chedid, E. (2019, January 21). New Lebanese law on e-transactions and data protection. Dentons. <https://www.dentons.com/en/insights/alerts/2019/january/21/new-lebanese-law-on-ettransactions-and-data-protection>

Coos, A. (2018, December 3). Data protection regulations in the Middle East. Endpoint Protector. <https://www.endpointprotector.com/blog/data-protection-regulations-middle-east/>

(2018) Data and privacy protection in ASEAN: What does it mean for businesses in the region? Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>

(2019, June). Data privacy frameworks in MENA: Emerging approaches and common principles,” GSMA and PWC. <https://www.gsma.com/mena/wp-content/uploads/2019/07/GSMA-Data-Privacy-in-MENA-Exec-Summary.pdf>

Değirmenci, N. (2016, April 8). Turkey’s First Comprehensive Data Protection Law Comes into Force. *Inside Privacy Blog*. Covington & Burling LLP. <https://www.insideprivacy.com/data-security/turkeys-first-comprehensive-data-protection-law-comes-into-force/>

DePalo, M. (2017, April 11). May 30 is fast approaching – are you ready for compliance with the amended Act on Protection of Personal Information in Japan? *Privacy & Cybersecurity Blog*. Alston & Bird. <https://www.alstonprivacy.com/may-30-fast-approaching-ready-compliance-amended-act-protection-personal-information-japan/>

Díaz Abreu, R. Employee data protection in Dominican Republic. Jiménez Cruz Peña. <https://www.lexology.com/library/detail.aspx?g=7ae40435-c721-4ca1-ace6-de3367769e84>

Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. Retrieved December 1, 2019, from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Data protection around the world. Commission Nationale de l’Informatique et des Libertés. Retrieved December 1, 2019, from <https://www.cnil.fr/en/data-protection-around-the-world>

Data protection laws of the world. DLA Piper. Retrieved December 1, 2019, from <https://www.dlapiperdataprotection.com/>

Enyew, A. B., (2016, December 2). Towards data protection law in Ethiopia. *Africa Data Privacy Laws*. 10.1007/978-3-319-47317-8_7

Greenleaf, G. (2014). Asian data privacy laws: trade and human rights perspectives. *Oxford University Press*.

Han, L. J. (2013, January 25). China’s legislature adopts decision on strengthening the protection of online information. *Global Privacy & Security Compliance Law Blog*. Latham & Watkins LLP. <https://www.globalprivacyblog.com/privacy/chinas-legislature-adopts-decision-on-strengthening-the-protection-of-online-information/>

Hannaford, G. (2018, September 6). Tajikistan: Data protection law ‘big step’ towards safety and security of personal data. OneTrust DataGuidance. <https://www.dataguidance.com/tajikistan-data-protection-law-big-step-towards-safety-and-security-of-personal-data-2/>

Hermansson, N., & Fussey, W. (2017, November 14). GDPR matchup: New Zealand's Privacy Act 1993. *IAPP*. <https://iapp.org/news/a/gdpr-matchup-new-zealands-privacy-act-1993/>

(2013, November 5). Kazakhstan enacts data privacy law. *Privacy & Information Security Law Blog*. Hunton Andrews Kurth. <https://www.huntonprivacyblog.com/2013/11/05/kazakhstan-enacts-data-privacy-law/>

Kennedy, G., & Lee K. (2019, January 9). Hong Kong: Change it up: Amendments to the Hong Kong Personal Data (Privacy) Ordinance being considered. *Mondaq*. <https://www.mondaq.com/hongkong/Privacy/769550/Change-It-Up-Amendments-To-The-Hong-Kong-Personal-Data-Privacy-Ordinance-Being-Considered>

Levac, L. (2015, December 11). Kuwait: Law regarding Electronic Transactions in force – introduction of a concept akin to data privacy. *Global Compliance News*. <https://globalcompliancenews.com/kuwait-law-regarding-electronic-transactions-in-force-introduction-of-a-concept-akin-to-data-privacy/>

Long, G. (2019, September 20). Ecuador fast-tracks data privacy law after massive breach. *Financial Times*. <https://www.ft.com/content/35f9aea0-dbb0-11e9-8f9b-77216ebe1f17>

Mohammed, B. (2019, June 22). Egypt's legislators pass country's first data protection regulation law. *Zawya*. https://www.zawya.com/mena/en/legal/story/Egyptys_legislators_pass_countrys_first_data_protection_regulation_law-SNG_147402777/

Moller, M. (2018). Data protection in Seychelles: Overview. *Practical Law*. <https://www.applebyglobal.com/publication-pdf/article/2018/data-protection-in-seychelles-overview.pdf>

Monteiro, R. L. (2018, August 15). The new Brazilian General Data Protection Law – a detailed analysis. *IAPP*. <https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>

Morgan, B. (2018, September 7). Barbados government publishes draft Data Protection Act. *IAPP*. <https://iapp.org/news/a/barbados-government-publishes-draft-data-protection-act/>

Moubaydeen, S. (2016, November 8). New national privacy law in Qatar. *Dentons*. <https://www.dentons.com/en/insights/alerts/2016/november/9/new-national-privacy-law-in-qatar>

Mulry, M., & Law J. (2019, August 15). Cayman Islands: Cayman Data Protection Law, 2017. *Mondaq*. <https://www.mondaq.com/caymanislands/Privacy/836816/Cayman-Data-Protection-Law-2017>

O'Donoghue, C. (2013, December 27). Kazakhstan introduces new privacy law. *Mondaq*. <https://www.mondaq.com/Privacy/283254/Kazakhstan-Introduces-New-Privacy-Law>

Olmos, K. A. (2019, April 4). Panama: New Law on Protection of Personal Data. *Mondaq*. <https://www.mondaq.com/Privacy/796006/New-Law-On-Protection-Of-Personal-Data>

Pattison, S. (2019, January 21). Which countries have the best cloud privacy laws in 2020? Cloudwards. <https://www.cloudwards.net/the-best-cloud-privacy-laws/>

(2018, May 9). Personal data protection guidelines for Africa. Internet Society and African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

(2012). Privacy and Data Protection: Assessment Report. International Telecommunications Union, HIPCAR. https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_assessment.pdf

(2015, May). Privacy and data protection laws of Bali Process member states. The Bali Process. <https://www.baliprocess.net/UserFiles/baliprocess/File/Privacy%20and%20data%20protection%20laws%20of%20Bali%20Process%20members%20States.pdf>

(2017). Privacy is paramount: Personal data protection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Rich, C. (2017, September 11). A look at new trends in 2017: Privacy laws in Africa and the Near East. *Bloomberg Law*. <https://media2.mofo.com/documents/170911-privacy-africa.pdf>

Rich, C. (2015, April 27). Privacy in Latin America and the Caribbean. *Bloomberg Law*. https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/PVRC/Privacy_Laws_Latin_America.pdf

Rich, C. (2016, June 24). Privacy laws around the world. *Bloomberg Law*. <http://garnerhealth.com/wp-content/uploads/2014/02/privacy-laws-around-the-world-report.pdf>

Rickett, D. (2011, May 3). Saudi Arabia: Data protection update 5 – Data protection in the Kingdom of Saudi Arabia. *Mondaq*. <https://www.mondaq.com/saudiarabia/Privacy/130992/Data-Protection-Update-5--Data-Protection-In-The-Kingdom-Of-Saudi-Arabia>

Ridgway, J., & Kelly, A. (2014, March 11). Australia: Data protection in the Pacific: What are your obligations? *Mondaq*. <https://www.mondaq.com/australia/Privacy/298520/Data-Protection-in-the-Pacific-What-are-your-obligations>

Saeed, M.A., & Muhammad, A.S. (2015, April). Cyber security and data privacy law in Saudi Arabia. *Financier Worldwide*. <https://www.financierworldwide.com/cyber-security-and-data-privacy-law-in-saudi-arabia#.XodpLqhKg2x>

Sanlate, G., Gordon, P., Martinez Méndez, S., & Varela, J.C. (2013, July 29). Colombia adopts regulations to implement its data protection laws. *Little*. <https://www.littler.com/publication-press/publication/colombia-adopts-regulations-implement-its-data-protection-laws>

(2019, November). Saudi Arabia: Data privacy landscape. *PwC*. <https://www.pwc.com/m1/en/services/tax/me-tax-legal-news/2019/saudi-arabia-data-privacy-landscape-ksa.html>

Schmidt, J. (2018, April 19). Costa Rica: Data privacy in Central America. *Mondaq*. <https://www.mondaq.com/Privacy/691118/Data-Privacy-In-Central-America>

Shyngyssov, A. (2013, July 2). Kazakhstan adopts personal data protection law. *Morgan Lewis*. https://www.morganlewis.com/pubs/ip_lf_kazakhstanadoptspersonaldataprotectionlaw_03july13

Simonova, V., Shapovalova, N. (2019, October 25). Amendments to the law on personal data in Kazakhstan: what does digitalization of the economy prepare for us? *Dentons*. <https://www.dentons.com/en/insights/alerts/2019/october/25/amendments-to-the-law-on-personal-data-in-kazakhstan>

(2018, May 8). St. Kitts and Nevis pass the Data Protection Bill 2018. *Privacy & Information Security Law Blog*. *Hunton Andrews Kurth*. <https://www.huntonprivacyblog.com/2018/05/08/st-kitts-nevis-pass-data-protection-bill-2018/>

Suwanprateep, D. (2019, March 1). Get ready: The first Thailand Personal Data Protection Act has been passed. *Baker McKenzie*. <https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data>

Sylla, A., & Ford-Cox, A. Overview of data protection laws in Africa. *Hogan Lovells*. <https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2>

- (2015, June). The right to privacy in Namibia. Privacy International. https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf
- (2018, April 16). The right to privacy in the digital age. Fiji Women's Rights Movement. <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/FWRM.pdf>
- (2016, March). The right to privacy in Venezuela. Acceso Libre, the International Human Rights Clinic at Harvard Law School, & Privacy International. https://hrp.law.harvard.edu/wp-content/uploads/2016/04/venezuela_upr2016.pdf
- (2016, March). The right to privacy in Zimbabwe. Zimbabwe Human Rights NGO Forum, Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School, & Privacy International. https://hrp.law.harvard.edu/wp-content/uploads/2016/04/zimbabwe_upr2016.pdf
- Tomaschek, A. (2019, October 9). Ecuador is in serious need of proper data protection laws following massive breach. Verdict. <https://www.verdict.co.uk/ecuador-data-protection-laws/>
- Warren, S., & Maakaron, C. (2017). Qatar's new Protection of Personal Data Privacy Law. Squire Patton Boggs. <https://www.squirepattonboggs.com/-/media/files/insights/publications/2017/11/qatars-new-protection-of-personal-data-privacy-law/28492--qatars-new-protection-of-personal-data-privacy-law.pdf>
- Webster, G., & Sacks, S. (2019, June 13). Five big questions raised by China's new draft cross-border data rules. *New America*. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-big-questions-raised-chinas-new-draft-cross-border-data-rules/>
- Wei, Y. (2018, February 7). Chinese data localization law: comprehensive but ambiguous. University of Washington. <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/>

APPENDIX B: ADDITIONAL CONTROL VARIABLES

TABLE 5: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF NATIONAL PRIVACY LAWS AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES EXPORTS (2005-2018)

VARIABLES	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects	(5) OLS	(6) Fixed Effects
<i>Law – Enacted</i>	0.306*** (0.0535)	0.0692 (0.0478)				
<i>Law – All Sectors</i>			0.497*** (0.0452)	0.0483 (0.0466)		
<i>Law – Data Adequacy</i>					0.469*** (0.0472)	0.0514 0.0473
<i>GDP (Log)</i>	1.026*** (0.0256)	0.67*** (0.0868)	0.979*** (0.0254)	0.6526*** (0.0853)	0.965*** (0.0273)	0.643*** (0.0867)
<i>Population (Log)</i>	-0.973*** (0.1426)	-0.497 (0.89)	-0.939*** (0.1433)	-0.455 (0.876)	-1.039*** (0.1452)	-0.446 (0.9512)
<i>Mobile Subscriptions (Log)</i>	-0.031 (0.0329)	0.1209** (0.0603)	-0.0405 (0.0335)	0.1402** (0.0628)	-0.0273 (0.0356)	0.175*** (0.062)
<i>Education (Log)</i>	0.0985 (0.0974)	0.2923* (0.1761)	0.0818 (0.0969)	0.1921 (0.1453)	0.0236 (0.1127)	0.1538 (0.1499)
<i>Labor Force (Log)</i>	0.7203*** (0.1326)	0.0621 (0.634)	0.773*** (0.1313)	-0.0989 (0.6451)	0.8435*** (0.1362)	0.028 (0.6609)
<i>Urban Population (Log)</i>	-0.0532 (0.064)	0.412 (0.5189)	-0.0839 (0.074)	0.5416 (0.5644)	-0.0538 (0.0755)	0.3655 (0.6235)
<i>Access to Electricity (Log)</i>	0.3379*** (0.064)	-0.2944 (0.2054)	0.415*** (0.0651)	-0.299 (0.2067)	0.438*** (0.066)	-0.333 (0.2162)
<i>Constant</i>	0.3419 (0.4203)	5.6863 (5.905)	0.3782 (0.0651)	6.3122 (5.8168)	0.9163 (0.444)	7.4233 (6.2038)
<i>Observations</i>	1,594	1,594	1,573	1,543	1,496	1,496
<i>R-squared</i>	0.8949	0.851	0.8953	0.8382	0.8883	0.8322
<i>F test</i>	2155***	48.77***	2211***	56.41***	1976***	52.41***
<i>Number of countries</i>		162		160		152

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

TABLE 6: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF NATIONAL PRIVACY LAWS AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES IMPORTS (2005-2018)

VARIABLES	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects	(5) OLS	(6) Fixed Effects
<i>Law – Enacted</i>	0.139*** (0.0308)	0.0371 (0.0500)				
<i>Law – All Sectors</i>			0.219*** (0.0273)	0.0277 (0.0550)		
<i>Law – Data Adequacy</i>					0.221*** (0.0286)	0.0150 (0.0551)
<i>GDP (Log)</i>	1.127*** (0.0199)	0.86*** (0.109)	1.109*** (0.0193)	0.850*** (0.112)	1.078*** (0.0195)	0.865*** (0.115)
<i>Population (Log)</i>	-0.0824 (0.0824)	-0.629 (1.041)	-0.129 (0.0846)	-0.380 (1.063)	-0.212** (0.0851)	-0.682 (1.166)
<i>Mobile Subscriptions (Log)</i>	0.086*** (0.0223)	0.00112 (0.0456)	0.0924*** (0.0217)	0.0161 (0.0487)	0.087*** (0.0236)	0.0233 (0.0485)
<i>Education (Log)</i>	-0.163** (0.0647)	0.0993 (0.151)	-0.196*** (0.0655)	0.0400 (0.145)	-0.126* (0.0744)	0.0140 (0.156)
<i>Labor Force (Log)</i>	-0.246*** (0.0787)	0.199 (0.416)	-0.128 (0.0818)	0.187 (0.426)	-0.0256 (0.0841)	0.285 (0.446)
<i>Urban Population (Log)</i>	-0.00467 (0.0413)	0.587 (0.597)	-0.0516 (0.0462)	0.404 (0.642)	-0.0423 (0.0474)	0.551 (0.722)
<i>Access to Electricity (Log)</i>	-0.304*** (0.0445)	-0.101 (0.129)	-0.253*** (0.0448)	-0.0856 (0.129)	-0.24*** (0.0460)	-0.122 (0.135)
<i>Constant</i>	1.101*** (0.283)	-1.020 (5.095)	1.103*** (0.292)	-1.590 (5.054)	1.160*** (0.308)	-0.650 (5.509)
<i>Observations</i>	1,591	1,591	1,570	1,570	1,493	1,493
<i>R-squared</i>	0.939	0.636	0.935	0.632	0.934	0.630
<i>F test</i>	3742***	51.8***	3696***	48.6***	3345***	53.6***
<i>Number of countries</i>		161		159		151

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

TABLE 7: LINEAR AND FIXED-EFFECTS REGRESSION MODELS OF MAXIMUM MONETARY PENALTIES AND DEMOGRAPHIC VARIABLES ON LOG COMMERCIAL SERVICES EXPORTS AND IMPORTS (2005-2018)

VARIABLES	<i>Exports</i>		<i>Imports</i>	
	(1) OLS	(2) Fixed Effects	(3) OLS	(4) Fixed Effects
<i>Maximum Monetary Penalty</i>	0.0313*** (0.00829)	0.0212*** (0.00672)	0.00955 (0.00690)	0.0225*** (0.00619)
<i>GDP (Log)</i>	1.266*** (0.0465)	0.653*** (0.0969)	1.277*** (0.0417)	0.965*** (0.0912)
<i>Population (Log)</i>	1.284*** (0.289)	-2.268 (2.110)	0.381* (0.209)	-1.007 (1.902)
<i>Mobile Subscriptions (Log)</i>	0.147* (0.0892)	0.107 (0.105)	0.261*** (0.0709)	-0.0610 (0.0759)
<i>Education (Log)</i>	0.195 (0.245)	0.215 (0.258)	0.0695 (0.166)	0.311 (0.333)
<i>Labor Force (Log)</i>	-1.464*** (0.262)	-0.564 (0.746)	-0.856*** (0.174)	-0.503 (0.608)
<i>Urban Population (Log)</i>	-0.465*** (0.135)	2.980* (1.510)	-0.0679 (0.129)	1.766 (1.490)
<i>Access to Electricity (Log)</i>	0.573*** (0.190)	-0.187 (0.416)	-0.682*** (0.114)	-0.464 (0.351)
<i>Constant</i>	-4.519*** (0.814)	4.078 (11.31)	0.0317 (0.683)	-4.520 (8.728)
<i>Observations</i>	448	448	448	448
<i>R-squared</i>	0.907	0.635	0.936	0.681
<i>F test</i>	723.2	29.24	1019	29.94
<i>Number of countries</i>		66		66

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

BIBLIOGRAPHY

- Cantwell, M. (2019, May 1). *Minority Statement in "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework."* Senate Committee on Commerce, Science, & Transportation. <https://www.commerce.senate.gov/2019/5/consumer-perspectives-policy-principles-for-a-federal-data-privacy-framework>
- Carson, A. (2018, August 28). Should vendors be able to pass along costs of GDPR compliance? *IAPP*. <https://iapp.org/news/a/should-vendors-be-able-to-pass-along-costs-of-gdpr-compliance/>
- Carlin, F. (1998, May). European privacy standards and their implications for international trade. *Journal of World Intellectual Property*.
- Chin, C. (2018, August 1). The U.S. privacy landscape post-GDPR. *Georgetown Public Policy Review*. <http://gppreview.com/2018/08/01/the-u-s-privacy-landscape-post-gdpr/>
- CIA World Factbook. Retrieved April 5, 2020, from <https://www.cia.gov/library/publications/the-world-factbook/geos/gm.html>
- Eger, J. M. (1978). Emerging restrictions on transnational data flows: privacy protection or non-tariff trade barriers? *Law & Policy in International Business*.
- Fefer, R. F. (2019, March 11). Data flows, online privacy, and trade policy. *Congressional Research Service*. <https://fas.org/sgp/crs/row/R45584.pdf>
- Fredriksson, T., Barayre, C., & Sinoncelli, O. (2016). Data protection regulations and international data flows: Implications for trade and development. UNCTAD. https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
- Kerry, C. F. (2016, November 9). Looking beyond transatlantic data transfers. *The Brookings Institution*. <https://www.brookings.edu/blog/techtank/2016/11/09/looking-beyond-transatlantic-data-transfers/>
- Kerry, C. F. (Forthcoming). America's privacy opportunity: The international stakes of United States privacy policy. *The Brookings Institution*.
- Madden, M., & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security, and surveillance. *Pew Research Center*. <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>
- Mattoo, A., & Meltzer J. P. (2018). International data flows and privacy: the conflict and its Resolution. *Journal of International Economic Law*, 21(4), 769-789. <https://doi.org/10.1093/jiel/jgy044>

- McGovern, G. (1977, June 9). The information age. *The New York Times*. <https://www.nytimes.com/1977/06/09/archives/the-information-age.html>
- Meltzer, J. P. (2014). The internet, cross-border data flows, and international trade. *Asia & the Pacific Policy Studies*, 2(1), 90-102. <https://doi.org/10.1002/app5.60>
- Muntermann, J., & Roßnagel, H. (2009). On the effectiveness of privacy breach disclosure legislation in Europe: empirical evidence from the US stock market. *NordSec. Lectures Notes in Computer Science*, 5838, 1-14. https://doi.org/10.1007/978-3-642-04766-4_1
- Mulligan, S. P., Freeman, W. C., & Linebaugh, C. D. (2019, March 25). Data protection law: An overview. *Congressional Research Service*. <https://fas.org/sgp/crs/misc/R45631.pdf>
- (2018, November 13). NTIA releases comments on a proposed approach to protecting consumer privacy. NTIA. <https://www.ntia.doc.gov/press-release/2018/ntia-releases-comments-proposed-approach-protection-consumer-privacy>
- Raul, A., Kerry, C. F., & Long, W. (2015, October 6). European Court of Justice strikes down U.S.-EU data transfer agreement. *The Brookings Institution*. <https://www.brookings.edu/blog/techtank/2015/10/07/european-court-of-justice-strikes-down-u-s-eu-data-transfer-agreement/>
- Roland-Holst, D., Evans, S., Behnke, D., Neal, S., Frölund, L., & Xiao, Y. (2019, August). Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations,” Berkeley Economic Advising and Research, LLC report prepared for the California Department of Justice. http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.
- Schapiro, G. (2018, April 18). *Testimony in “Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy.”* House Committee on Oversight and Reform, Subcommittee on Information Technology. <https://oversight.house.gov/legislation/hearings/subcommittee-on-information-technology-hearing-game-changers-artificial-1>
- Sedgewick, M. B. (2017). Transborder data privacy as trade. *California Law Review*, 105(5), 1513-1542. <https://dx.doi.org/10.15779/Z382V2C94C>
- Shaffer, G. (2000). Globalization and social protection: the impact of EU and international rules in the ratcheting up of U.S. privacy standards. *Yale Journal of International Law*, 25(1). <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1112&context=yjil>
- Swire, P. P. (1998). Of elephants, mice, and privacy: international choice of law and the internet.

International Lawyer, 32(4), 991-1025. <https://www.jstor.org/stable/40707456>

Whitman, J. Q. (2004, April). The two western cultures of privacy: dignity versus liberty. *Yale Law Journal*.

https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers