WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 12, ISSUE 1 FALL 2016

PRIVACY HARMONIZATION AND THE DEVELOPING WORLD: THE IMPACT OF THE EU'S GENERAL DATA PROTECTION REGULATION ON DEVELOPING ECONOMIES

Tiffany Curtiss, CIPP/US[*]

CITE AS: 12 WASH. J.L. TECH. & ARTS 95 (2016)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1654

ABSTRACT

Through strengthened third-party obligations for data protection, the European Union's General Data Protection Regulation will export privacy norms. However, developing economies may want to consider a co-regulatory industry approach to data protection before adopting similar national legislation. The General Data Protection Regulation can be an ideal model for global harmonization of privacy laws, particularly for adoption among industries and willing participants. To benefit from a co-regulatory approach, however, a developing economy would need to invest in education and legal systems in order to capture the benefits of the growing e-commerce market that will undoubtedly be influenced by the General Data Protection Regulation.

[*] Tiffany Curtiss, University of Washington School of Law, Class of 2017.

TABLE OF CONTENTS

INTRODUCTION

In January 2012, the European Union ("EU") released a new proposal for data protection that would replace the 1995 Data Protection Directive.[1] This proposal, also known as the General Data Protection Regulation ("GDPR"), was adopted in April 2016.[2]

---

[1] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (2012) 11 final, (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

[2] Regulation 2016/679 (EU) of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, hereinafter "GDPR Final Text," *available at* http://eur-lex.europa.eu/legal-

The GDPR represents the next wave of data protection reform that will strengthen compliance by third-party subcontractors with whom data is shared. The GDPR replaces the Data Protection Directive 95/46/EC (the "Directive"), which was created to harmonize data privacy laws across the EU member states. Given the significant technological changes since the Directive was passed in 1995, the GDPR seeks to preserve EU harmonization while modernizing data privacy laws. The GDPR includes assurances that citizens who provide their information with informed consent will have their information protected even when that information is shared with third parties. While the GDPR still requires EU member states to enact harmonizing national legislation, it improves upon the 1995 Directive by strengthening protections for individual rights and increases the power of the European Commission over those of national data protection commissions. By May 2018, all member states will have nationalized the requirements of the GDPR.[3]

Through strengthened third-party obligations for data protection, the European Union's GDPR will result in the exportation of privacy norms. However, developing economies may want to consider a co-regulatory industry approach to data protection before adopting similar national legislation. Part I of this Article explains the history and of data privacy law in the European Union. Part II discusses how the GDPR can lead to the adoption of data privacy practices in countries without comprehensive data privacy laws through the private sector. Part III identifies challenges for developing economies to adopt a comprehensive regime like the GDPR, and proposes co-regulatory approach for data privacy.

I. THE EUROPEAN UNION AS A LEADER IN PRIVACY AND SECURITY REGULATION

Soon after the 'big data' phenomenon and rise of massive

content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL.

[3] *Id*.

global data collectors enabled by the Internet, privacy became a major concern among many Western nations. European officials were quick to respond to growing concerns regarding big data and privacy with sweeping data protection laws adopted in 1995. Speculations arose that the EU would become the driver of international privacy norms.[4] For example, in 2001, Joel Reidenberg, a law professor at Fordham University, testified before the House Committee on Energy and Commerce that "[i]n effect, Europe through the European Directive has displaced the role that the United States held since the famous Warren and Brandeis article in setting the global privacy agenda."[5] Today, the European Union has arguably emerged as a leader in the fight to preserve traditional norms of individual privacy in the digital age. If any nation—or, as in this case, group of nations—can be effective at exporting its privacy norms across the globe, it will likely be the EU.

Until the mid-nineties, each of the EU member states had unique national privacy legislation.[6] However, under this model, efforts within individual countries to ensure privacy for their citizen's data could easily be undermined when that data was transferred to other member states with weaker data protection regulations. This prompted the EU to attempt to harmonize data protection with omnibus privacy laws.[7] Unlike the United States,

---

[4] *See, e.g.*, *The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearings Before the Subcomm. On Commerce, Trade, and Consumer Protection*, 107th Cong., at http://www.house.gov/commerce/hearings/03082001-49reidenberg104/htm (2001) (testimony of Prof. Joel Reidenberg).

[5] *Id.*

[6] *See, e.g.*, Jeffrey B. Ritter, et al., *Emerging Trends in International Privacy Law*, 15 Emory Int'l L. Rev. 87, 90–91 (2001) ("The genesis of modern legislation in this area can be traced to the first data protection law in the world, enacted in the Land of Hesse in Germany in 1970. That enactment was followed by national laws with differing objectives and scope in Sweden (1973), the United States (1974), Germany (1977), and France (1978).").

[7] Directive 95/46 1995 O.J. (L 218) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

which regulates data protection from a sector approach,[8] the EU's omnibus approach was intended to establish standards for information law broadly.

In 1995, the European Parliament adopted the EU Data Protection Directive[9] with two major objectives: (1) to protect the fundamental right to data protection; and (2) to guarantee the free flow of personal information between member states.[10] This latter goal enabled the European Union to achieve greater harmonization of data protection by requiring that each Member State enact national legislation to protect "the fundamental rights and freedoms of natural persons . . . ."[11] The Directive requires any EU-based company to comply with specific rules for processing and transferring European consumer data and further grants those consumers certain rights and controls with regards to their personal data, such as the right to be notified of all uses and disclosures about data collection and processing, and the right to correct or delete personal data.

The Directive imposes certain privacy requirements on those who would collect consumer data. It requires, for example, that companies protect personal information with adequate security, and companies can only transfer data to other countries with an "adequate level of protection."[12] This means that European companies seeking to utilize third-party services in another country need to ensure that equivalent privacy and security are implemented by the third-party company in order to transfer personal data outside of Europe.

Since the adoption of the Data Protection Directive, the EU has passed other complementary directives that further address the

---

[8] Peter P. Swire & Kenesa Ahmad, Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices 32 (Terry McQuay ed., 2012).

[9] Directive 95/46 1995 O.J. (L 218) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[10] *Id.*

[11] *Id.*

[12] *Id.* at art. 25.

collection and use of personal information issues aggravated by new technologies. The Directive on Privacy and Electronic Communications was established in 2002 to address protections in electronic mail, telephone communication, traffic data, caller ID, and spam.[13] This directive was then altered by the Data Retention Directive, which set out minimum and maximum retention schedules for data.[14] The 2009 Amendment Directive, also known as the Cookie Directive, required that opt-in consent be given for the use of cookies on a website.[15]

II. THE NEW GENERAL DATA PROTECTION REGULATION WILL PUSH EU PRIVACY NORMS TO NON-EU COUNTRIES VIA THE PRIVATE SECTOR.

In January 2012, the EU released a new proposal for data protection that would replace the 1995 Data Protection Directive.[16] The GDPR was adopted in April 2016.[17] The GDPR represents the next wave of data protection reform that will strengthen compliance by third-party subcontractors with whom data is shared. The GDPR replaces the Data Protection Directive 95/46/EC (the "Directive"), which was created to harmonize data privacy laws across the member states of the European Union. Given the significant technological changes since the Directive

---

[13] Directive 2002/58, 2002 O.J. (L 200) (EC) on Privacy and Electronic Communications, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24120.

[14] Directive 2006/24, 2006 O.J. (L 105) (EC), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024.

[15] Directive 2009/136, 2009 O.J. (L 337) (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

[16] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (2012) 11 final, (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

[17] *See* GDPR Final Text at art. 44.

was passed in 1995, the GDPR seeks to preserve EU harmonization while modernizing data privacy laws. The GDPR includes assurances that citizens who provide their information with informed consent will have their information protected even when that information is shared with third parties.[18] While the GDPR still requires EU member states to enact harmonizing national legislation, it improves upon the 1995 Directive by strengthening protections for individual rights and increases the power of the European Commission over those of national data protection commissions. By May 2018, all member states will have nationalized the requirements of the GDPR.[19]

A. Binding Corporate Rules and Model Clauses

A chief provision of the GDPR is that EU rules must apply if personal data is handled abroad by companies that actively offer services to EU citizens or render services to entities in the EU.[20] Today, data can comply with European data privacy laws by requiring contractual commitments from subcontractors to maintain a reasonable level of security, employ industry standard security practices, and obey all applicable data security laws. This approach has been accepted under EU law because current regulations permit the transfer of personal data to third-party countries that do not have an "adequate level of protection" if the protection of privacy and individual freedoms "result from appropriate contractual clauses."[21]

Companies subjected to EU data protection laws have taken three main approaches: (1) adopting binding corporate rules ("BCRs"); (2) signing standard contractual clauses also known as Model Clauses; and (3) waiting for the Privacy Shield, which will

---

18 *Id.* ("Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.").

19 *Id*. at art. 51.

20 *Id* at chapter V.

21 Directive 95/46/EC, Art. 26(2).

replace the Safe Harbor a new self-certification regime for data transfers to U.S. processors. For example, in the wake of the U.S.-EU Safe Harbor invalidation,[22]U.S. a few companies implemented BCRs or signed Model Clauses in an effort to continue doing business with EU customers and partners.[23]

Reliance on BCRs and Model Clauses has not been widely adopted, even by those seeking an alternative to the Safe Harbor. Fewer than a hundred companies globally have sought to have their BCRs approved by a national data protection authority.[24] This is partly due to the time, expense, and effort it takes to get approval.[25] Due to the uncertainty regarding safeguards sufficient to permit cross-border data transfers—aggravated by the invalidation of the Safe Harbor—even data protection authorities are taking a wait-and-see approach until there is clear guidance on how to comply.[26]

---

[22] *See* Press Release, Court of Justice of the European Union, *The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*, Court of Justice of the European Union (Oct. 6, 2015), *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[23] *See, e.g.*, Ancestry.com, *Ancestry EU Safe Harbor - Privacy Shield Update*, *available at* http://www.ancestry.com/cs/legal/ancestry-eu-safe-harbor-privacy-shield (last visited Aug. 12, 2016); *see also* Daniel Alvarez, *Safe Harbor Is Dead; Long Live the Privacy Shield?*, Bus. L. Today, May 2016, at 1, 4 ("Consequently, companies that have been using Safe Harbor must analyze and implement alternative mechanisms going forward, at least until a new agreement is reached.").

[24] *See* European Commission, *List of companies for which the EU BCR cooperation procedure is closed*, European Commission – Justice (last accessed May 22, 2016), *available at* http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

[25] *See* Phillip Rees et al., *Transferring Personal Data Outside the EEA: The Least Worst Solution*, 13 Computer and Telecommunications Law Review 66 (2007).

[26] *See, e.g.*, Mark Young & Monika Kuschewsky, *EU Data Protection Authorities Enforcement Guidance Post-Schrems*, National Law Review, Feb. 21, 2016 ("Senior officials within the Swedish Data Protection Authority are reported to have put in place an informal enforcement moratorium, the duration of which is uncertain as 'for the moment [the Swedish Data Protection Authority

Compliance with the GDPR will likely still rely on contractual commitments as a main mechanism to enforce EU privacy regulations abroad.[27] As such, European data controllers (i.e. the companies collecting consumer information) are encouraged to require non-EU processors (e.g. subcontractors) to sign data protection commitments that have been approved by an EU member state's data protection authority.[28] The GDPR does this by officially recognizing the use of BCRs and Model Clauses as appropriate safeguards: "[s]uch appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorized by a supervisory authority."[29]

B. Enhanced Administrative Fines

Apart from its formal recognition of the use of approved BCRs and Model Clauses as appropriate safeguards, the GDPR differs from 1995 Data Protection Directive in its increase in the size of monetary sanctions for violations.[30] For example, severe breaches may be subjected to fines of "up to 4% of worldwide turnover."[31] For companies such as Google and Facebook, violations of the GDPR could be a large as €460 million ($516 million) and €2.3 billion ($2.6 billion), respectively.[32] In addition,

---

is] not taking any such action.'").

[27] *See* Manu J. Sebastian, *The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises?*, 31 Syracuse J. Sci. & Tech. L. Rep. 216, 242–43 (2015).

[28] *See* Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 Berkeley J. Int'l L. 939, 993 (2006).

[29] GDPR Final Text, Clause 108.

[30] *See id.* at Art 83.

[31] James Drury-Smith et al., *Two Years to Get Ready – GDPR Adopted*, JD Supra (Apr. 15, 2016), *available at* http://www.jdsupra.com/legalnews/two-years-to-get-ready-gdpr-adopted-56868/.

[32] Cyrus Farivar, *EU agrees on new law that severely punishes firms for*

each supervisory data authority would have the power to impose administrative fines and would not be preempted by a fine imposed by another authority. The GDPR outlines multiple factors that should aid an authority when determining the appropriate administrative fine. In the end, however, that the fine is required only to be "effective, proportionate and dissuasive."[33]

For the GDPR to be effective in exporting data protection standards, companies will need to believe that data protection authorities are actively imposing fines or other sanctions. If companies believe that enforcement is rare, or occurs only in cases of severe data breaches, companies may feel taking the risk of enforcement is not worth the investment into strengthened data protection. Respect for the GDPR is critical to effectuate the desired level of protection of an individual's information and harmonizing global privacy laws. The downstream privacy and security obligations will encourage compliance as a selling point, and therefore stimulate investment in data protection.[34] This could create market competition and so motivate other companies to also implement privacy practices into their operations. However, if the private sector does not believe in the GDPR's enforcement, or if there is a respected dissent against the GDPR that creates uncertainty of its shelf-life, the pressure to ensure third-party compliance will remain lax and largely on paper.

With data collectors bearing more risk for the activities of their subcontractors, the GDPR may have the effect of exporting European privacy norms through the private sectors seeking to do

---

violating user privacy, ARS TECHNICA UK (Dec. 16, 2015), *available at* http://arstechnica.co.uk/tech-policy/2015/12/tech-firms-could-owe-up-to-4-of-global-revenue-if-they-violate-new-eu-data-law/.

[33] GDPR Final Text, Article 83.

[34] World Economic Forum & Accenture, Digital Transformation of Industries: Digital Enterprise, Geneva: World Economic Forum (Jan. 2016, 12), *available at* http:// reports.weforum.org/digital-transformation-of-industries/ wp-content/blogs.dir/94/mp/files/pages/files/digital-enterprisenarrative-final-january-2016.pdf ("The growing use of data will create new opportunities for businesses in fields such as data analysis, data transparency and cybersecurity. It will also require higher levels of investment in data security by those companies collecting, storing and analyzing consumer data.").

international business.

III. A MODEL FOR DEVELOPING ECONOMIES?

The question underlying the GDPR and its downstream impact on data processors is whether its data protection standards should serve as a model for non-EU countries, particularly developing countries without established or robust privacy regimes. To answer this question, we must consider the pros and cons of the comprehensive approach taken by the EU embodied in the GDPR, as well as the realities common among developing countries, such as potential resources for enforcement.

Four major models for data protection are commonly used around the world; comprehensive, sectoral, self-regulatory, and technology-based.[35] Comprehensive data protection laws govern the collection, use, and dissemination of personal information in both the public and private sectors.[36] The sectoral framework protects personal information by enacting laws that address a particular industry sector, such as medical records and credit records.[37] The self-regulatory model emphasizes the creation of codes of practice for the protection of personal information by a company, industry or independent body.[38] The technology-based model uses technical measures as alternative protections that reduce the relative importance of administrative measures for overall privacy protections such as encryption.[39]

The EU has used the comprehensive model since its 1995 adoption of the Data Protection Directive, and has continued this approach in the GDPR. The primary benefit of a comprehensive approach is its installation of an official agency or commissioner responsible for overseeing enforcement, also known as a data

---

[35] Swire, *supra* note 6.

[36] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Land and Developments*, 18 J. Marshall J Computer & Info L. 1 (Fall 1999).

[37] *See* Pub. L. No. 104-191 (1996) (Health Insurance Portability and Accountability Act); Pub. L. No. 91-508 (1970) (Fair Credit Reporting Act).

[38] An example of a self-regulatory model is the Payment Card Industry Data Security Standard (PCI DSS) which outlines measures for cardholder data security.

[39] Swire, *supra* note 6 at 34.

protection authority.[40] The data protection authority is also generally responsible for educating the public on data protection and also acts as an international liaison for data protection matters.[41]

However, the comprehensive approach is not without its critics.[42] The three main criticisms of the one-size-fits all model are: (1) the costs of the regulations can outweigh the benefits, (2) the same level of strictness may not be justified for all types of data, and relatedly, (3) a comprehensive regime may stifle innovation.[43]

A. Challenges with a comprehensive approach to privacy

For developing countries, the costs alone may undermine the integrity of adopting the regulations under the GDPR.[44] These costs will come in the form of cyber liability insurance and the tools and effort to comply with "consent, data mapping and cross-border transfer requirements."[45] Even if a country were to adopt comprehensive data protection laws, they might lack the resources to implement and enforce those laws. Resources would be needed to fund the enforcing body as well as its costly paperwork, documentation, auditing, and other requirements. Cost burdens would affect not only the government but any and all companies subject to the regulations. At a minimum, companies would be required to have a designated representative to respond to privacy

---

40 *Id.* at 31.

41 *Id.*

42 *See* The European Privacy Officers Forum, Comments on Review of the EU Data Protection Directive (Directive 95/46/EC) (Jul. 31, 2002) *available at* http://www.epof.org/files/Uploads/Documents/EPOF/EPOF_en2_7.31.02.pdf.

43 *Id.*

44 *See* Data Privacy Survey: GDPR Costs and Complexity a Concern, Barker Makenzie (May 4, 2016), *available at* http://www.bakermckenzie.com/en/newsroom/2016/05/data-privacy-survey-gdpr-costs-and-complexity.

45 *Id.*

requests and conduct self-assessments.[46] As mentioned above, regulations can only be effective if those regulated believe there is meaningful enforcement. Therefore, developing countries with budgetary restraints may not have the fiscal means to meet their desired privacy ends.

Another key consideration for developing economies is the barrier to innovation that privacy regulations may present to burgeoning industries. Similar to the tensions with the use of controversial energy sources,[47] the use of big data spurs tensions between developed and developing economies.[48] For example, companies such as Google and Facebook, established in the United States, have undoubtedly flourished from their use of user data. Anyone seeking to develop a product that utilizes predictive algorithms[49] that are necessarily based on the processing of personal data would be hard-pressed to succeed under a comprehensive privacy regime; particularly against competitors operating in jurisdictions without broad regulations on data use.

B. Weaknesses for developing economies

Apart from the challenges imposed by a comprehensive approach to privacy, developing nations may also be ill-equipped to meet GDPR expectations. Developing nations are more likely to lack technical sophistication, national privacy regimes, or effective judicial systems. These shortcomings would represent significant weaknesses for protecting personal information in the data-sharing chain.[50]

---

[46] GDPR Final Text, Art. 27.

[47] *See* E.A. Wrigley, ENERGY AND THE ENGLISH INDUSTRIAL REVOLUTION (2010).

[48] Rosemary Wyber et al., *Big data in global health: improving health in low- and middle-income countries*, World Health Organization (Jan. 30, 2015), *available at* http://www.who.int/bulletin/volumes/93/3/14-139022/en.

[49] Predictive algorithms enable more tailored servicing often associated with efficiency and product quality. *See generally* Pedro Domingos, The Master Algorithm (2015).

[50] Swire, *supra* note 6.

Many developing economies have capitalized on low labor costs in providing competitive business process outsourcing for companies. Developing and emerging nations striving to be premier business process outsourcers are eager to meet the demand from the growing tech sector. Many companies have taken advantage of differences in labor costs and have chosen to outsource business processes such as customer service functions to developing nations. These processes often require at least minimal access to customer information.[51]

1. Technical Inferiority

Technical inferiority is a major hurdle for data processing companies in developing countries.[52] Often this stems from either a lack of local technical education opportunities or from a migration of skilled labor—known as a "brain drain"—of a country's educated youths.[53] Even developed nations like the United States suffer from a shortage of privacy professionals, and training/certification organizations have been growing in an effort to meet this need.[54] For example, the International Association of Privacy Professionals was established in 2000 and now boasts over 3,100 individuals holding the Certified Information Privacy Professional for the United States (CIPP/US) credential.[55] However, even this amount falls behind in comparison to the more-than-4,000 organizations that have workers who are self-certified under the EU-US Safe Harbor agreement for trans-

---

[51] *See* Timothy Morey et al., Customer Data: Designing for Transparency and Trust, Harvard Business Review, May 2015, *available at* https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[52] Swire, *supra* note 6.

[53] *See*, Sunita Dodani & Ronald E LaPorte, Brain drain from developing countries: how can brain drain be converted into wisdom gain?, J. R. Soc. Med. 98, Nov. 2005, 487–491.

[54] *See About the IAPP: The world's largest global information privacy community*, International Association of Privacy Professionals ([DATE LAST UPDATED/VISITED HERE], *available at* https://iapp.org/about/.

[55] *Id.*

continental data transfers. Under a comprehensive model, encompassing every organization that collects personal information including employee data, it would be difficult for the United States to meet the privacy professional need, let alone a developing nation without equivalent educating bodies.

Similarly, privacy in today's digital world essentially requires technical knowledge of industry standard security practices.[56] Despite administrative measures such as privacy policies for organizational guidance, technical measures are a key ingredient to sufficient data protection. For some developing countries, this can be a challenge.[57] When a population lacks reliable access to safe housing, clean water, and health services, education and investment in cybersecurity training are lesser priorities. For example, many college students in Kenya only have access to computers or internet via their universities; those students who attend universities without those resources must often resort to internet cafes where usage is charged by the minute.[58]

However, it is important to acknowledge the spectrum of developing economies and their varying abilities to have a technically educated workforce. Romania, for example, is known for producing strong computer science students and is also considered a developing economy by the International Monetary Fund.[59] However, a challenge for Romania is keeping their talent within its borders, even as a Member State of the EU. Brain drain is a major issue for countries like Romania that invest in education, but lack the private-sector strength to employ recent graduates.[60]

---

[56] For example, ISO 27001 and NIST SP 800-53 are two internationally recognized information security standards which organizations can audit and certify practices against.

[57] *See* ISO and IEC Developing Country Assistance Efforts, ANSI, August 2005.

[58] This is noted from the author's personal experience in 2007 in Nairobi, Kenya among students at the University of Nairobi and Kenyatta University.

[59] International Monetary Fund, *Uneven Growth: Short- and Long- Term Factors,* WORLD ECONOMIC OUTLOOK (Apr. 2015), *available at* http://www.imf.org/external/pubs/ft/weo/2015/01/pdf/text.pdf

[60] Marian Chiriac, *Romania Fears Brain Drain as Students Head Abroad*, BALKAN INSIGHT, Sept 15, 2015, available at

However, the demand for stronger data protection could arguably provide an opportunity for countries that are developed enough in the education sector to mitigate some losses associated with brain drain. According to one Romanian technology journalist, several companies "plan to increase their Romanian teams by up to 20 percent this year . . . . because security officers are easier to find there, compared with Western Europe . . . . [and] skills are competitively priced."[61]

Similarly, companies may even prefer to be under the authority of developing countries that have security expertise but lack a strong technology industry because they may be more business-friendly. Like countries that promote themselves as tax havens, countries which curate political pressure to attract and keep private sector business may offer more lenient enforcement of the data protection regulations.[62] Technical education remains important because data protection authorities will still need to be able to understand how a company's technology works to avoid arbitrary determinations.

However, an obvious risk with choosing a developing country as an enforcing authority may be a lack of political stability and an abundance of corruption. As such, inferiority in technical education can make the GDPR an unsavory option for developing countries because companies would not be able to find the necessary talent to comply with the GDPR. As a result, such companies may opt to avoid such local markets. Nevertheless, the GDPR may offer an opportunity to position a developing country as a desirable location to anchor a regional business hub, despite technical inferiority. Companies could prioritize competent

---

http://www.balkaninsight.com/en/article/many-romanian-students-want-to-study-abroad-09-24-2015

[61] Andrada Fiscutean, *Demand for security skills is ballooning: So can former hacker hotbed Romania help?*, ZDNET Mar. 8, 2016, *available at* http://www.zdnet.com/article/demand-for-security-skills-is-ballooning-so-can-former-hacker-hotbed-romania-help.

[62] *See, e.g.*, Witold J. Henisz & Bennet A. Zelner, The Hidden Risks in Emerging Markets, Harv. Bus. Rev. (Apr. 2010).

employees and regulators thirsty for foreign investment. By adopting the GDPR, a developing country could become an approved nation for international data transfers.

2. Unsophisticated Judicial Regimes

A comprehensive data protection model would designate an agency or commissioner as the enforcement mechanism. As previously discussed, developing economies have some desirable attributes to companies—typically cost-competitive labor and accommodating government incentives. However, developing economies are often also characterized by underdeveloped legal regimes. While this will not necessarily be a barrier to adopting the GDPR as a model for national data protection laws, it is likely to significantly impact the benefits that would flow from it.

Under the GDPR, data subjects would need meaningful access to a remedy for privacy violations. However, the judicial processes of a country seeking to comply with the GDPR for purposes of data transfers from other EU countries could undermine the private sector's efforts. Judicial redress for data subjects, for example, was a primary reason behind the invalidation of the US-EU Safe Harbor agreement.[63] The EU Commission found that there was insufficient access to the courts under U.S. law.[64] Since the invalidation, the United States Congress has sought to remedy this gap through legislation.[65] In doing so, however, Congress has yet to mitigate another large concern: government surveillance.

Developing countries without a sophisticated legal regime are likely to find it difficult to meet the judicial requirements. Private sector companies in developed countries that have not been

---

[63] *See* Natasha Lomas, *Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S.*, TechCrunch (Oct. 6, 2015), *available at* https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s.

[64] *Id.*

[65] *See* Client Alerts, *US House Passes Judicial Redress Act to Facilitate Safe Harbor Negotiations*, Cooley LLP (Oct. 23, 2015), *available at* https://www.cooley.com/us-judicial-redress-act-to-facilitate-safe-harbor-negotiations.

approved for data transfers, or countries seeking to perform data processing services for international companies, will need to rely on the use of binding corporate rules or model clauses.[66]

The private sector's reliance on contract law raises another issue regarding unsophisticated judicial regimes. Without a sophisticated judicial structure, contract breach claims could suffer from extreme delays and complicated administrative bureaucracies.[67] Notorious for extreme delays among developing economies is India. Economist Matthieu Chemin of McGill University investigated the impact of India's speed in closing cases and its impact on the Indian economy.[68] Under his calculations, "[i]n India, it takes an average of 2 years to dispose of any case. . . . Extreme examples of judicial slowness refer to cases taking 47 years to be resolved by which time the plaintiff had died."[69] Chemin's results indicated that "the speed of courts across Indian states plays an important role in shaping economic activity in this important sector of the economy."[70] Important to note, however, is the impact that an amendment[71] to India's Code of Civil Procedure had on improving efficiency and decreasing contract breaches in the country. These changes improved the efficiency of the court by decreasing the number of cases pending per judge and the average

---

66 GDPR Final Text, Clause 108.

67 *See, e.g.*, Witold J. Henisz & Bennet A. Zelner, The Hidden Risks in Emerging Markets, Harv. Bus. Rev. (Apr. 2010); *see also* Matthieu Chemin, *Does Court Speed Shape Economic Activity? Evidence from a Court Reform in India*, Nov. 11, 2010, J. Law Econ. Organ., *available at* http://matthieuchemin-research.mcgill.ca/research/1%20Chemin%202012%20JLEO.pdf

68 Matthieu Chemin, *Does Court Speed Shape Economic Activity? Evidence from a Court Reform in India*, J. Law Econ. Organ., Nov. 11, 2010, *available at* http://matthieuchemin-research.mcgill.ca/research/1%20Chemin%202012%20JLEO.pdf.

69 *Id.* at 6 (citing Krishnamoorty, Dasu, Judicial Delays, Indolink, editorial analysis, 2003).

70 *Id.* at 24.

71 The Code of Civil Procedure (Amendment) Act, 2002 Act NO. 22 of 2002, (May 23, 2002).

case duration.[72] Chemin's research found that speedier courts "decrease[] the probability to experience a breach of contract, increases investment, and decrease[] the probability to experience a shortage of capital."[73]

Developing countries that fail to recognize the importance of judicial efficiency will, in effect, only harm the data processing companies that exist within their borders and strive to be compliant with the GDPR through contractual means. Further, by having a legal system that does not provide avenues for redress for foreign citizens, efforts to harmonize with the EU's GDPR will remain incomplete. Thus, developing countries would be unable to benefit from its adoption.

3. Eagerness to grow

However, a developing country's eagerness to grow could harm its efforts to harmonize with the GDPR if that eagerness outweighs its efforts to implement data protection measures.[74] This could take place at either the governmental or private sector levels. If a government becomes too eager to tout itself as progressive on privacy in an effort to look modernized, or to attract business without following through, for example, then it is unlikely to be deemed compliant as an EU data protection /authority.[75] This would create the same results as having an unsophisticated judiciary.[76] Further, eagerness from the private sector to commit to security promises and practices without substantial compliance could put not only the company, but the country at reputational

---

72 Chemin, *supra* note 67 at 24.

73 *Id*.

74 Swire, *supra* note 6.

75 *See* GDPR Final Text, Clause 103.

76 *See, e.g.*, Witold J. Henisz and Bennet A. Zelner, *The Hidden Risks in Emerging Markets*, Harvard Business Review, April 2010. *See also* Matthieu Chemin, Does Court Speed Shape Economic Activity? Evidence from a Court Reform in India, J. Law Econ. Organ., Nov. 11, 2010, *available at* http://matthieuchemin-research.mcgill.ca/research/1%20Chemin%202012%20JLEO.pdf.

risk. [77]

In a free market, businesses will typically seek to provide services that are better, faster, or cheaper. This in turn benefits the consumer. However, when it comes to data protection, it is not as easy to recognize when data protection commitments are being kept. The majority of consumers only learn that a trusted organization has not kept up their end of the bargain when a data breach occurs, spilling personal information onto the internet.[78] More often than not, consumers in developing countries are wholly unaware of the nature of their actual data processors, who are often third parties outsourced to a more reputable company. Vague and overly broad privacy notices generally extend to allow the sharing of personal data to third parties when necessary to provide services,[79] and cost considerations may motivate outsourcing business processes, such as customer service, to countries with lower labor costs.

In such a race to the bottom on margins, data processors in low-cost labor markets would not be incentivized to go above the bare minimum necessary to do business. Data security is not cheap. It requires the employment of at least one skilled technician, and under the GDPR, compliance can be costly.[80] As seen in the U.S.-EU Safe Harbor program, the ability to self-certify compliance was previously an acceptable means of compliance.[81] Under the Safe

---

[77] *See* Matthieu Chemin, Does Court Speed Shape Economic Activity? Evidence from a Court Reform in India, J. Law Econ. Organ., Nov. 11, 2010, 4, *available at* http://matthieuchemin-research.mcgill.ca/research/1%20Chemin%202012%20JLEO.pdf.

[78] *See* Dana Tamir, *How a Third-Party Data Breach Leads Hackers to Your Data*, Security Intelligence, (Feb. 5, 2014), *available at* https://securityintelligence.com/how-a-third-party-data-breach-leads-hackers-to-your-data.

[79] *See, e.g.*, Microsoft's Privacy Statement, Reasons We Share Personal Data, *available at* https://privacy.microsoft.com/en-us/privacystatement ("We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized.").

[80] *See supra* Part III.A.

[81] *See* Information Required for Safe Harbor Self-Certification,

Harbor, companies based in the United States needed only to self-certify that they implemented the necessary technical and administrative safeguards to adequately protect the privacy principles of the EU Data Protection Directive.[82] Indeed, the only requirement was a self-certified statement that the subcontractors had sufficient security measures in place. It was not required to seek more from subcontracted data processors. A comprehensive data security assessment with an audit in the United States can cost $48,000 on average for the data collector themselves.[83] As a result, trying to extend this level of independent review was often costly for companies, developing country or not. The further down the data-sharing chain a data processor lies, the less likely that the accountability of a data protection regime will come in to verify security commitments; particularly when the data processor is in a different country than the original data controller subjected to the data protection regulations.[84]

This diminishing verification and accountability structure can create a similar result as having lax enforcement mechanisms.[85] Weighing the cost against the risk, data processors may take the gamble. While such behavior is in no way unique to developing economies, reputational harm would probably be more dramatic for countries trying to gain a market share in business process outsourcing. While consumers may not care where the leak came from, data controllers who hire the data processors will lose trust in the industry. Consumers' perceptions of an industry's quality will matter in the local economy because they have the

---

Department of Commerce, *available at* http://2016.export.gov/safeharbor/eu/eg_main_018491.asp.

82 *Id.*

83 *See* John Verry, *ISO-27001 Cost Estimate: $48,000 Information Security Confidence: Priceless*, PivotPoint Security (July 26, 2012), *available at* http://www.pivotpointsecurity.com/blog/iso-27001-cost-estimate-48000-information-security-confidence-priceless.

84 *See* Natalie Kim, *Three's A Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 Harv. J.L. & Tech. 325, 340 (2014) ("The additional step down the chain, to the second node, erodes accountability and enforceability, delaying regulatory progress in this area.").

85 *Id.*

purchasing power. Just as China battles against issues regarding the reputation of its product quality,[86] developing countries in the data processing industry may similarly develop reputations for being secure only on paper. This, in turn, is likely to hurt the companies who are legitimately implementing compliant data protection programs.

As companies seek to reduce costs, the data protections may decrease in quality if investments in data security are reduced. As discussed in Part II.B., enforcement will be key to compliance. The GDPR can be a powerful catalyst to enabling foreign investment if companies in developing countries offer low-cost, compliant services. Given its reliance on self-certification and the large cost to verify compliance, however, the quality assurances could be merely representations without actual implementation of security measures. On the other hand, if a national government were to adopt and enforce national laws in line with the GDPR, their enforcement could enable competition among secure solutions.

4. Risk of exploitation

Developing economies seeking to gain positions as trusted data processors may also risk exploitation by more sophisticated organizations. Companies more experienced in contract law—either by virtue of being located in more legally sophisticated jurisdictions or that have superior bargaining power—can take advantage companies in developing countries, particularly with pass-through terms that would effectively lay liability for data loss or leaks on the data processor.[87] While this would only be the case if the data processor were actually to blame, previous discussion has noted the diminishing incentive to ensure compliance. As such,

---

[86] *See, e.g.*, *Poorly Made: Why so many Chinese products are born to be bad*, The Economist (May 14, 2009), *available at* http://www.economist.com/node/13642306.

[87] *See* John Ahlquist & Aseem Prakash, *FDI and the Costs of Contract Enforcement in Developing Countries*, Policy Sciences 43, no. 2 (2010) 181-200.

this could result in half-hearted efforts to put pressure on actual compliance beyond contractual protections.

The GDPR seeks to close this exploitation of pass-through data protection commitments by holding the data controller liable for the breaches of their data processors in cases where the enforcing data protection authority determines that the controller failed to adequately ensure compliance beyond mere contractual commitments.[88]

This change in data protection law will undoubtedly increase accountability among data controllers and data processors in turn. Although a data controller may seek to recover costs associated with a breach from subcontractors, controllers will be incentivized to ensure compliance with contractual commitments from the outset, or to contract with subcontractors in countries with reliable judicial regimes where they are more likely to successfully recover.

C. A Co-Regulatory Approach

Given the costs and broad protections of the GDPR, the best approach for a developing country is likely to be a co-regulatory model. A co-regulatory model emphasizes industry development of enforceable standards for privacy and data protection against a backdrop of legal requirements by the government.[89] This approach would be similar to the self-regulatory approach, in that the regulations would be driven by the industry most affected by international data protection laws. However, the co-regulatory model would add assurance to data controllers by having the government acknowledge a breach of those standards as a contract breach.[90] This could show a developing country's commitment to an industry without having to stifle innovation in other areas.

A co-regulatory approach would also be more efficient to implement, since standards would be set by those with expertise in

---

88 GDPR Final Text, Article 28(4).

89 Swire, *supra* note 6.

90 *Id.*

the regulated area instead of relying on government bodies that may lack technical skills and knowledge of the area. This particularly parallels aspects from the sectoral approach used in the United States by picking and choosing important industries,[91] but unlike the United States, would not be significantly retarded by government inaction to stay up to date with technological advances.[92]

The GDPR could be an ideal model for global harmonization of privacy laws, particularly for adoption among industries and willing participants. However, to benefit from a co-regulatory approach, a developing economy would need to invest in education and legal systems in order to capture the benefits of the growing e-commerce market.[93]

CONCLUSION

The European Union's new GDPR will inevitably export privacy norms beyond the borders of the EU. In the absence of government regulation, the private sector will become the leading source of privacy norms in industries that collect personal data, setting a baseline for competition as well as consumer expectations. Given the ease with which personal data can now be shared across country borders and the benefits that can arise from aggregated data, having consistent protections for personal data throughout the data processing lifecycle will allow for more e-commerce opportunities and increased consumer protection.

Developing countries with the ability to educate their youths have the opportunity to benefit from increasing data security needs globally, and these benefits can be increased if the country has a trustworthy, pro-business government and an efficient judiciary. However, if a government continues to struggle with education, corruption, or inefficient courts, then adopting a comprehensive privacy or data security regime could hurt even the

---

91 *See supra* note 37.

92 Swire, *supra* note 6.

93 *See* Part II.B(1).

well-meaning private sector organizations striving to participate in international e-commerce. A co-regulatory approach would be an intermediate step towards a comprehensive model that allows a nation to roll out a regime with less risk.

PRACTICE POINTERS

- Developing countries seeking to ensure an adequate level of protection essentially equivalent to that of the EU should evaluate whether they have the capacity to independently supervise data protection and provide effective and enforceable rights through effective administration and judicial redress.
- Data processing companies in non-EU countries should consider adopting binding corporate rules or standard contractual clauses.
- EU data controllers should perform due diligence of privacy and data security measures for all data processors beyond contractual commitments to follow GDPR requirements.