

INTERNATIONAL

August 2019

EXPECT FOCUS[®]

LEGAL ISSUES AND DEVELOPMENTS FROM CARLTON FIELDS

REGULATIONS RISING REGULATORY IMPACT AND STAYING AFLOAT



**CARLTON
FIELDS**

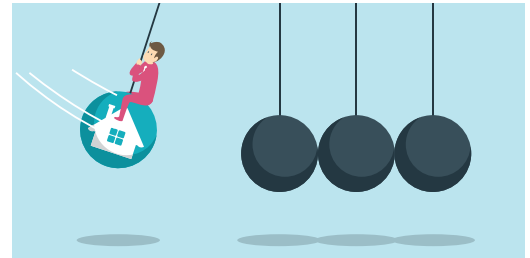
3 The Practical Effect of Blocking Statutes on Helms-Burton Title III Actions



4 Regulating Privacy on the Blockchain Starts With Understanding the Meaning of “Personal Data”



6 FIRRMA Impact on Real Estate Transactions



EXPECTFOCUS[®]

INTERNATIONAL, AUGUST 2019

Executive Editor Andrew J. (Josh) Markus

Editor Barry Leigh Weissman

Production Manager Jessica Bennett

Art Director & Designer Frances Liebold

Contributors Steven Blickensderfer
Brian Hart
Justin Wales

EXPECTFOCUS[®] International is a review of legal issues and developments related to international business, provided on a complimentary basis to clients and friends of Carlton Fields.

The content of EXPECTFOCUS[®] is for informational purposes only and is not legal advice or opinion. EXPECTFOCUS[®] does not create an attorney-client relationship with Carlton Fields or any of its lawyers.

SUBSCRIPTIONS: Changes in address or requests for subscription information should be submitted to: Peggy Bourque, pbourque@carltonfields.com.

Copyright © 2019 Carlton Fields. All rights reserved. No part of this publication may be reproduced by any means, electronic or mechanical, including photocopying, imaging, facsimile transmission, recording, or through any information storage and retrieval system, without permission in writing from Carlton Fields. EXPECTFOCUS[®] is a registered trademark of Carlton Fields.



The Practical Effect of Blocking Statutes on Helms-Burton Title III Actions

BY ANDREW J. (JOSH) MARKUS

There has been a lot of anticipation in various communities, both positive and negative, about what will happen when litigation under Title III of the Helms-Burton Act becomes a reality. In fact, it is a reality, but not everything is positive for claimants in such litigation. One obstacle to be considered is the so-called blocking statutes that have been enacted by various governments. This article is presented to provide some background on the practical effect of these statutes.

When the Helms-Burton Act (the Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996), 22 U.S.C. §§ 6021-6091, was enacted, Title III permitted legal action against people and entities who “trafficked” in property confiscated by the Cuban government. The word “trafficking” was so broadly defined as to encompass anything that anyone could have done in connection with property in Cuba. The scale of expropriation was also so broad that virtually any property in Cuba would be considered off limits to ownership, use, or development of any type.

Many nations were aghast at the audacity of the scope of Title III. They have long considered the extraterritorial application of U.S. laws excessive. To combat its extraterritorial effect, they passed “blocking statutes.” These statutes permit a national of the applicable country who is subjected to Title III liability to sue the Title III litigant for damages in the defendant’s home

country. In addition, the blocking statutes mandate that a judgment obtained under Title III not be enforced in the defendant’s home country. Besides these rights, the blocking statutes almost uniformly prohibit compliance with the Helms-Burton prohibitions, including requests by the courts of the United States.

What is the practical effect of a blocking statute? First, venue of Title III litigation will almost always need to be in the United States. Second, Title III litigation will only be effective if assets of the defendant are in the United States. Third, the Title III plaintiff cannot have assets in the defendant’s country. Fourth, if witnesses or documents are required to be obtained from the defendant outside the United States, any subpoena or other request will not be honored.

In the case of the recent litigation commenced by the U.S.-citizen heirs of Rafael Lucas Sánchez Hill against the Meliá hotel chain, the European Union has threatened to use the EU blocking statute (Council Regulation (EC) No. 2271/96 of 22 November 1996 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom) as well as asserting its rights under the World Trade Organization for sanctions against the United States. The EU blocking regulation applies to any individual or entity that is an EU national or that is

incorporated in the EU. Accordingly, in the 28 countries comprising the EU (27 after Brexit), any pursuit of compensation will be blocked from enforceability, and if the plaintiff has a presence or assets in the EU, it and they will be at risk.

Finally, while this article has concentrated on the problems the plaintiff will have in pursuing a Title III claim, it should be noted that blocking statutes place people and entities with a presence in the United States and assets in the United States between a rock and a hard place. Under the blocking statutes, the defendant violates its own law by complying with U.S. court orders. If the U.S. court levies sanctions as a result, the defendant may consider that it has no choice but to comply in the United States.

As more cases are filed, the U.S. effects of Title III will become clearer. At the moment, it remains unclear if Title III will be able to be practically enforced except in specific, narrowly defined fact situations and only against U.S. defendants.

Regulating Privacy on the Blockchain Starts With Understanding the Meaning of “Personal Data”

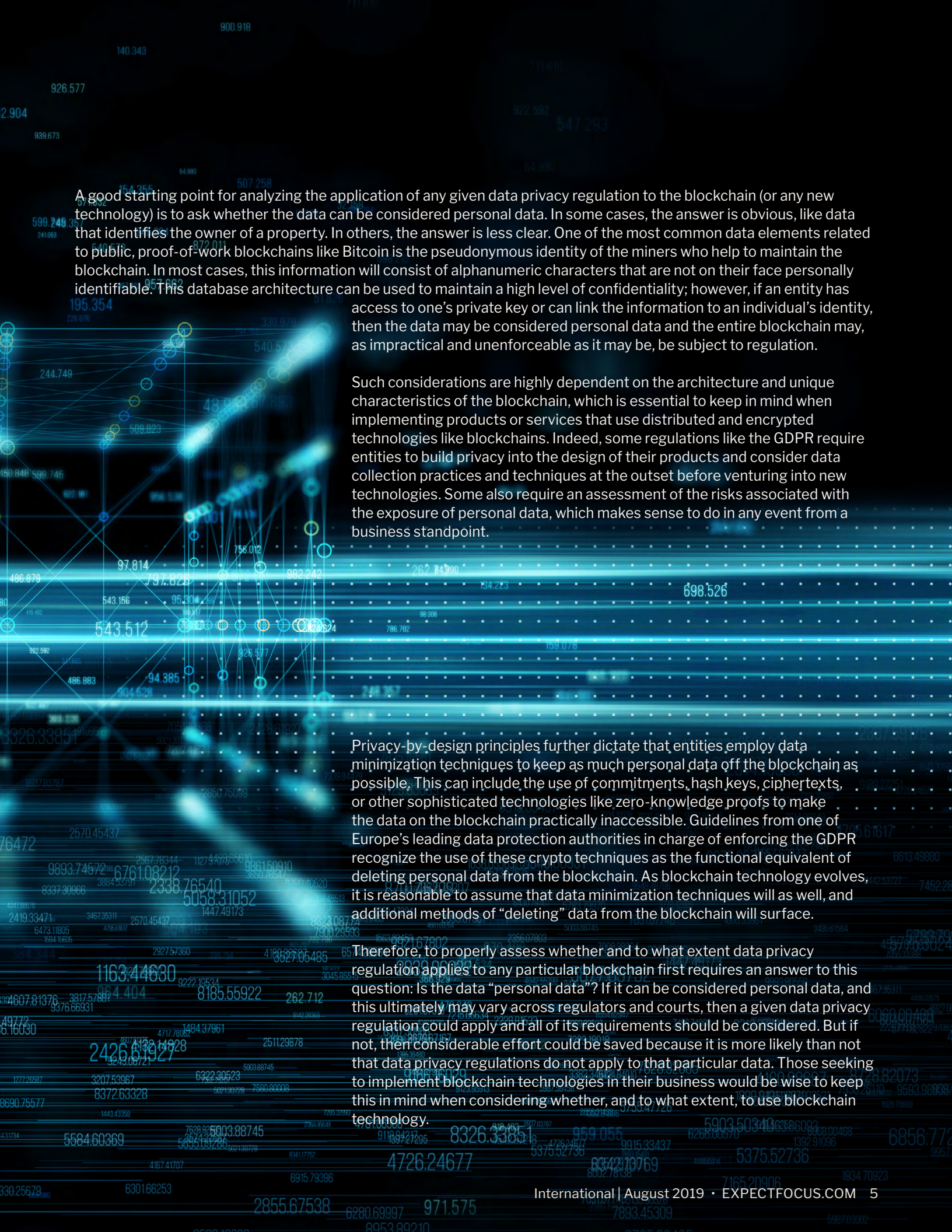
BY STEVEN BLICKENSDECKER & JUSTIN WALES

A commonality among recent data privacy regulations (including the EU’s GDPR, California’s CCPA, and Brazil’s LGPD) is that only the storage and transmittal of “personal data” is regulated. These new regulatory frameworks generally define “personal data” (or “personal information”) obliquely as elements that relate, by themselves or taken together with other data, to an identified or identifiable individual. As companies across the world explore transitioning data storage onto encrypted, open databases including blockchains or similar technologies, an emerging question has arisen over whether such uses could violate privacy regulations and, counterintuitively, force companies into adopting less secure data storage methods than available through new technologies.

Part of the challenge of applying new technologies to existing regulatory frameworks is definitional. Privacy regulations purposefully employ broad definitions of “personal data” that make it difficult to apply to all types of data. Excluded from most regulations are business-to-business data (B2B), data used solely for household purposes, and “anonymous data,” meaning data that has had personal identifiers removed or rendered indecipherable. The exact bounds of these categories remain unclear, and it is not often easy to categorize data as fitting into one category to the exclusion of other regulated data types.

Privacy regulations are generally technology agnostic and apply to all methods of storage and transmittal, including blockchains. One of the challenges of applying privacy regulations to blockchains is that not all blockchains are equal or employ the same level of security or encryption. Some have open, decentralized, and pseudonymous characteristics, and therefore may or may not be compatible with regulatory frameworks.

Generally, regulators have treated blockchain technologies like cloud computing and view it as just an additional means of collecting and processing data. Accordingly, if data on a particular blockchain cannot be used to identify an individual, then it is generally spared from data privacy regulation altogether. The same is true for data contained on a public, permissioned, or private blockchain.



A good starting point for analyzing the application of any given data privacy regulation to the blockchain (or any new technology) is to ask whether the data can be considered personal data. In some cases, the answer is obvious, like data that identifies the owner of a property. In others, the answer is less clear. One of the most common data elements related to public, proof-of-work blockchains like Bitcoin is the pseudonymous identity of the miners who help to maintain the blockchain. In most cases, this information will consist of alphanumeric characters that are not on their face personally identifiable. This database architecture can be used to maintain a high level of confidentiality; however, if an entity has access to one's private key or can link the information to an individual's identity, then the data may be considered personal data and the entire blockchain may, as impractical and unenforceable as it may be, be subject to regulation.

Such considerations are highly dependent on the architecture and unique characteristics of the blockchain, which is essential to keep in mind when implementing products or services that use distributed and encrypted technologies like blockchains. Indeed, some regulations like the GDPR require entities to build privacy into the design of their products and consider data collection practices and techniques at the outset before venturing into new technologies. Some also require an assessment of the risks associated with the exposure of personal data, which makes sense to do in any event from a business standpoint.

Privacy-by-design principles further dictate that entities employ data minimization techniques to keep as much personal data off the blockchain as possible. This can include the use of commitments, hash keys, ciphertexts, or other sophisticated technologies like zero-knowledge proofs to make the data on the blockchain practically inaccessible. Guidelines from one of Europe's leading data protection authorities in charge of enforcing the GDPR recognize the use of these crypto techniques as the functional equivalent of deleting personal data from the blockchain. As blockchain technology evolves, it is reasonable to assume that data minimization techniques will as well, and additional methods of "deleting" data from the blockchain will surface.

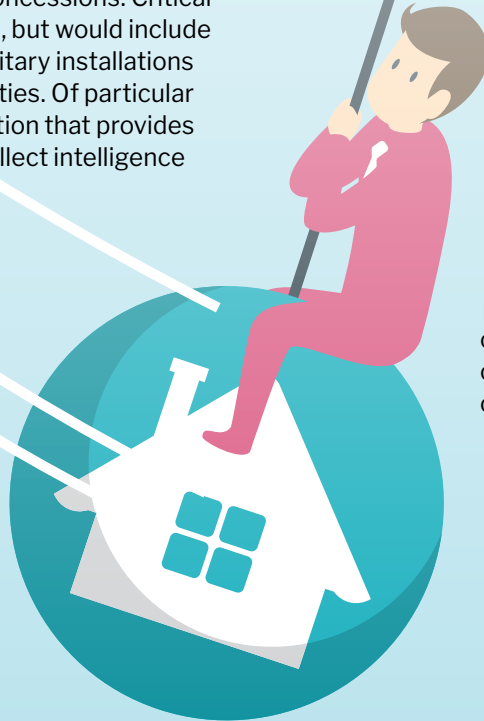
Therefore, to properly assess whether and to what extent data privacy regulation applies to any particular blockchain first requires an answer to this question: Is the data "personal data"? If it can be considered personal data, and this ultimately may vary across regulators and courts, then a given data privacy regulation could apply and all of its requirements should be considered. But if not, then considerable effort could be saved because it is more likely than not that data privacy regulations do not apply to that particular data. Those seeking to implement blockchain technologies in their business would be wise to keep this in mind when considering whether, and to what extent, to use blockchain technology.

FIRRMA Impact on Real Estate Transactions

BY BRIAN HART

Covered Transactions

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) now specifically brings real estate transactions directly under the jurisdiction and review of the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee created to review the national security impacts of foreign investments in the United States. CFIUS is empowered to block or impose measures to reduce any threats to U.S. national security. Covered transactions include the purchase, lease, or concession by or to a foreign person of developed or undeveloped land in close proximity to critical infrastructure. The expansion to undeveloped land is a significant change, as purely “greenfield” investments will now be subject to CFIUS review. A concession is not defined, but presumably would include arrangements for the operation of real estate, such as parking concessions. Critical infrastructure is broadly defined, but would include airports, maritime ports, and military installations and other U.S. government facilities. Of particular concern to CFIUS is any transaction that provides a foreign person the ability to collect intelligence or surveillance on the activities being conducted at any of these facilities. For example, CFIUS recently required the Chinese conglomerate HNA Group to sell its stake in a New York City building whose tenants included the police precinct protecting Trump Tower.



What Steps Should Be Taken to Comply With the New Law?

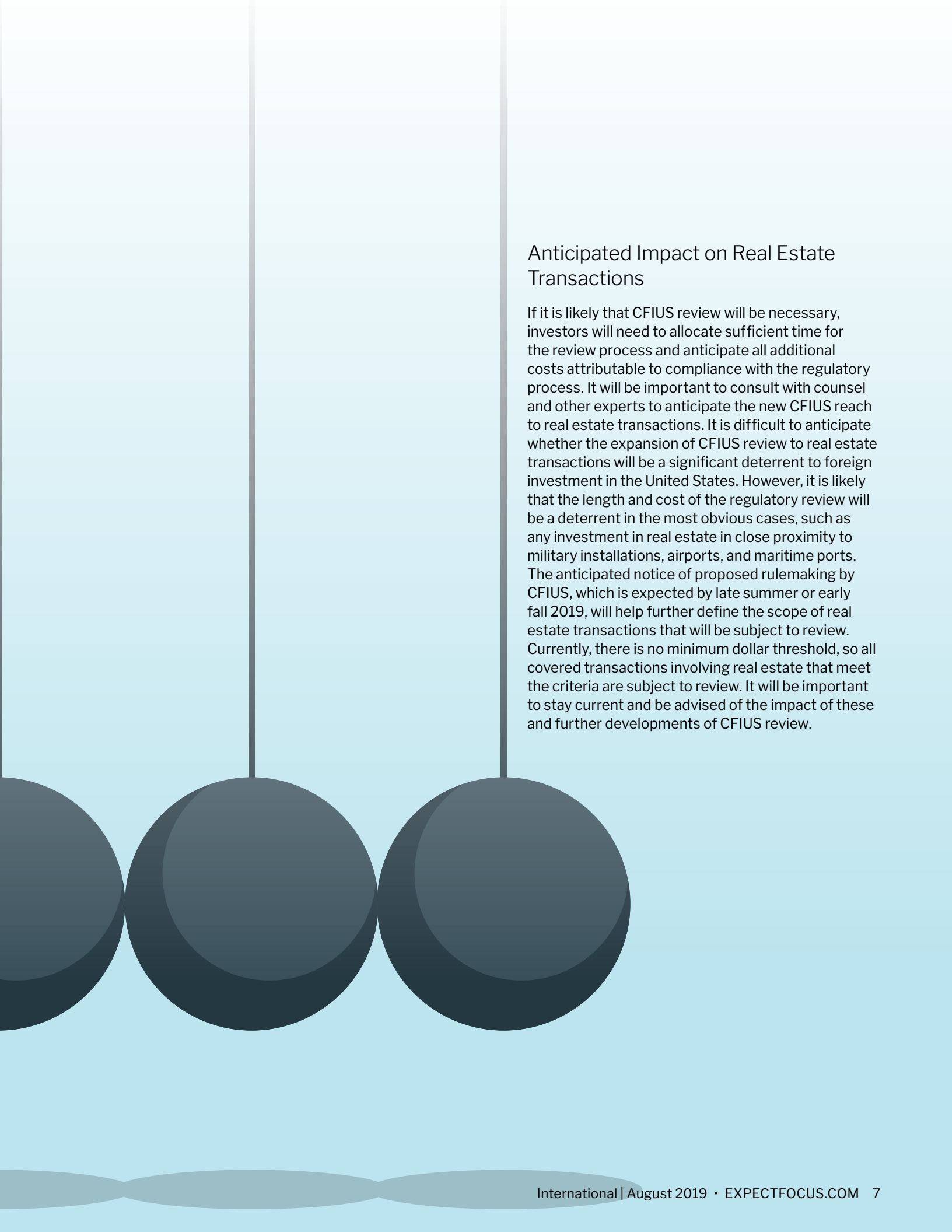
First, you must know the identity of all investors to determine if a proposed investment could be subject to CFIUS review. A “foreign person” includes a foreign entity.

Second, you must determine if a proposed property is in close proximity to critical infrastructure. Close proximity is not currently defined, but is subject to definition by further regulations by CFIUS.

Third, you should determine whether to voluntarily submit a short form filing (“declaration”) that will provide basic information regarding the transaction. CFIUS is then required to determine if a full formal filing is necessary within 30 days following the receipt of a declaration. If you decide to submit a formal filing, FIRRMA provides a 45-day review period, with an optional 45-day investigation period and a one-time extension beyond that time frame of 15 days in “exceptional circumstances.” FIRRMA authorizes CFIUS to charge a filing fee of up to 1% of the transaction or \$300,000, whichever is less.

What Is Not Covered

Covered transactions would not include the purchase of a “single housing unit,” certain real estate in urbanized areas, or passive investments. Passive foreign investment in equity funds are not included when the funds are managed by a U.S. person and foreign investors are limited from impacting investment decisions. Loans secured by real property are not considered covered transactions, unless the foreign person acquires economic or governance rights characteristic of an equity investment and not a loan.

A Newton's cradle with five spheres is shown in the background. The spheres are dark grey and are suspended by thin vertical lines. The background is a light blue gradient. The text is positioned to the right of the cradle.

Anticipated Impact on Real Estate Transactions

If it is likely that CFIUS review will be necessary, investors will need to allocate sufficient time for the review process and anticipate all additional costs attributable to compliance with the regulatory process. It will be important to consult with counsel and other experts to anticipate the new CFIUS reach to real estate transactions. It is difficult to anticipate whether the expansion of CFIUS review to real estate transactions will be a significant deterrent to foreign investment in the United States. However, it is likely that the length and cost of the regulatory review will be a deterrent in the most obvious cases, such as any investment in real estate in close proximity to military installations, airports, and maritime ports. The anticipated notice of proposed rulemaking by CFIUS, which is expected by late summer or early fall 2019, will help further define the scope of real estate transactions that will be subject to review. Currently, there is no minimum dollar threshold, so all covered transactions involving real estate that meet the criteria are subject to review. It will be important to stay current and be advised of the impact of these and further developments of CFIUS review.



CARLTON FIELDS serves business clients in key industries across the country and around the globe. Through our core practices, we help our clients grow their businesses and protect their vital interests. The firm serves clients in the following key industries:

Banking, Commercial, and Consumer Finance
Construction
Health Care
Life, Annuity, and Retirement Solutions

Property and Casualty Insurance
Real Estate
Securities & Investment Companies
Technology & Telecommunications

For more information, visit our website at www.carltonfields.com.

Atlanta

One Atlantic Center
1201 W. Peachtree Street NW
Suite 3000
Atlanta, Georgia 30309-3455
404.815.3400 | fax 404.815.3415

Hartford

One State Street | Suite 1800
Hartford, Connecticut 06103-3102
860.392.5000 | fax 860.392.5058

Los Angeles

2000 Avenue of the Stars
Suite 530, North Tower
Los Angeles, California 90067-4707
310.843.6300 | fax 310.843.6301

Miami

Miami Tower
100 S.E. Second Street | Suite 4200
Miami, Florida 33131-2113
305.530.0050 | fax 305.530.0055

New Jersey

180 Park Avenue | Suite 106
Florham Park, New Jersey 07932-1054
973.828.2600 | fax 973.828.2601

New York

Chrysler Building
405 Lexington Avenue | 36th Floor
New York, New York 10174-3699
212.785.2577 | fax 212.785.5203

Orlando

SunTrust Center – Main Tower
200 S. Orange Avenue | Suite 1000
Orlando, Florida 32801-3400
407.849.0300 | fax 407.648.9099

Tallahassee

215 S. Monroe Street | Suite 500
Tallahassee, Florida 32301-1866
850.224.1585 | fax 850.222.0398

Tampa

Corporate Center Three
at International Plaza
4221 W. Boy Scout Boulevard | Suite 1000
Tampa, Florida 33607-5780
813.223.7000 | fax 813.229.4133

Washington, D.C.

1025 Thomas Jefferson Street, NW
Suite 400 West
Washington, DC 20007-5208
202.965.8100 | fax 202.965.8104

West Palm Beach

CityPlace Tower
525 Okeechobee Boulevard | Suite 1200
West Palm Beach, Florida 33401-6350
561.659.7070 | fax 561.659.7368