

In this issue:

Message From the Chair.....	5
From the Editors.....	10
Access Wars: How the Second Circuit’s Opinion in <i>Microsoft v. United States</i> Changes the Rules for Government Access to Data in Cross-Border Investigations.....	12
When You Have Suffered a Data Breach, Attribution May Be Useful, But Hacking Back? Not So Much!	14
Duty Free? The Effect of International Data Privacy and Protection Laws on Employers’ Ability to Monitor Business Emails of Employees Working Outside the United States	16
Protecting Corporate Trade Secrets From Former Employee ‘Haccess’	18
The EU’s Attempt at a Comprehensive Approach to Regulation and Enforcement of Data Protection.....	20
Cybersecurity: A Sea Change in Maritime Commerce.....	22
International Legal Assistance and Special Considerations Presented in the Cybercrime Context.....	24
Internet Regulation and Data Protection: The Role of Law Enforcement	26
Homeland Security and Data Privacy: A Primer on Customs’ Global Entry Program	28
Feeling Pushed Up Against the Wall? Current U.S. Immigration Climate Demands That U.S. Employers ‘Think Outside the Box’	30
Worksite Enforcement: An Attorney’s Role in Counseling Employers About the I-9 Audit Process and E-Verify.....	32
The Bitter Side of <i>Ius Pecuniae</i> in the United States: The Risks Facing EB-5 Investors	37
The Impact of International and U.S. Domestic Law on the Future of the Global Medical Marijuana Market.....	41
World Roundup	46
Section Scene	52



International Law Section Leadership

Alvin F. Lindsay III	Chair
Eduardo Palmer	Immediate Past Chair
Arnoldo B. Lacayo	Chair-Elect
Carlos F. Osorio	Secretary
Clarissa A. Rodriguez	Treasurer
Angie Froelich	Program Administrator

International Law Quarterly

Rafael R. Ribeiro	Editor-in-Chief
Javier Peral	Editor
Loly Sosa	Editor
Susan Trainor	Copy Editor
Colleen Bellia	Graphic Designer
Clarissa A. Rodriguez	Advertising crodriguez@tenzer.com

This publication is prepared and published by The Florida Bar.

Statements or opinions or comments appearing herein are those of the editors and contributors and not of The Florida Bar or the International Law Section.

Articles may be reprinted with permission of the editor and the author(s) of the requested article(s).

Contact: Rafael Ribeiro at rafael.ribeiro@hoganlovells.com



Features

12 • Access Wars: How the Second Circuit's Opinion in *Microsoft v. United States* Changes the Rules for Government Access to Data in Cross-Border Investigations

The U.S. Department of Justice has continued to pursue appeals in *Microsoft v. United States*, and lower courts in at least two other circuits have disagreed with the ruling. Companies now confront multiple standards governing how to comply with government-initiated requests for company data. This article provides a practical examination of these recent developments and suggestions for how companies should react to these changes.

14 • When You Have Suffered a Data Breach, Attribution May Be Useful, But Hacking Back? Not So Much!

Company executives may ask questions such as these when a data breach occurs: What can we do to get our data back, or at least disable or destroy the perpetrator's ability to attack us? This article provides guidance on what to do—and what not to do—when faced with a data breach.

16 • Duty Free? The Effect of International Data Privacy and Protection Laws on Employers' Ability to Monitor Business Emails of Employees Working Outside the United States

This article follows George Que's travels while on a business trip to Canada, the United Kingdom, Germany, Japan, and Australia to illustrate how the data privacy laws of these countries can affect a U.S. company's legal rights to access its employees' emails.

18 • Protecting Corporate Trade Secrets From Former Employee 'Haccess'

Too often, terminated or disgruntled employees seek to extract vital information from a corporation for personal gain. This article discusses ways that a company can protect confidential information as well as actions that can be taken against a former employee who hacks into a corporate database, drive, or cloud information system.

20 • The EU's Attempt at a Comprehensive Approach to Regulation and Enforcement of Data Protection

The European General Data Protection Regulation (GDPR) will come into force throughout the European Union on 25 May 2018. This article offers an overview of the history and key components of the GDPR, as well as some comments on how it might fare as an attempt to stem the rising tide of cyberbreaches.

22 • Cybersecurity: A Sea Change in Maritime Commerce

Reliance on technology in the maritime industry requires that ship owners, ship charterers, and marine insurers make adequate preparations to ensure that the electronic information and communication systems that underpin the maritime industry are protected from compromise by a cybersecurity event. This article summarizes steps being taken to prevent cyberbreaches at sea.

24 • International Legal Assistance and Special Considerations Presented in the Cybercrime Context

This article discusses the interplay between Mutual Legal Assistance Treaties (MLATs) and search warrants, as well as the possibility that recent changes to Fed. R. Crim. P. 41's search warrant provisions for computers and electronically

stored information may support similar changes to 18 U.S.C. § 3512's current constraint on the manner in which a U.S. court addresses a foreign state's MLAT request for a Rule 41 search warrant.

26 • Internet Regulation and Data Protection: The Role of Law Enforcement

One of the most interesting themes encountered when undertaking research about cyberspace concerns its regulation in regard to civil society and law enforcement. This article includes a brief history of cyberlibertarianism and its decline, and then offers an explanation of cyberpaternalism and network communitarianism, two theoretical points of view on cyberspace.

28 • Homeland Security and Data Privacy: A Primer on Customs' Global Entry Program

This article describes eligibility requirements for membership in the U.S. Customs and Border Protection's Global Entry program, the benefits of membership, how to apply for membership, and how one can challenge any denial or revocation of membership.

30 • Feeling Pushed Up Against the Wall? Current U.S. Immigration Climate Demands That U.S. Employers 'Think Outside the Box'

This article discusses increased scrutiny of both the H-1B and L-1 visa classifications by U.S. government agencies involved in their processing, due to perceptions of abuse over the last several years. The authors foresee this trend continuing, particularly in light of the Trump administration's stance on immigration, and discuss innovative strategies employers may use to navigate current trends.

32 • Worksite Enforcement: An Attorney's Role in Counseling Employers About the I-9 Audit Process and E-Verify

The author examines the consequences of recent immigration enforcement actions for U.S. employers and how attorneys can help them comply with established laws and regulations in order to limit the employers' civil and criminal liability. The article also examines the pros and cons of the E-Verify program for employers.

37 • The Bitter Side of *Ius Pecuniae* in the United States: The Risks Facing EB-5 Investors

U.S. lawmakers are taking aim at the EB-5 program as it currently exists. Some seek to eliminate the program in its entirety while others seek to increase the investment requirement while adding fraud prevention and recovery mechanisms. This article summarizes the challenges EB-5 investors face and discusses possible solutions.

41 • The Impact of International and U.S. Domestic Law on the Future of the Global Medical Marijuana Market

As of the 2016 election cycle in the United States, medical marijuana is legal in twenty-eight states and is quickly moving toward legalization in all fifty states. In light of the lack of a national approach for legalization, the author discusses three major hurdles that may impede the international growth of the industry.



THE FLORIDA BAR
INTERNATIONAL LAW SECTION



Thank You to our 2016-2017 Annual Sponsors

GLOBAL SPONSORS



WWW.ABALLI.COM



WWW.HOGANLOVELLS.COM

HEMISPHERIC SPONSORS



REGIONAL SPONSORS



Message From the Chair

The Section's Historic Trip to Havana

"Only oppression should fear the full exercise of freedom." José Martí

"Ladies and gentlemen, your flight time today will be forty-eight minutes." When the captain made that announcement, most of us were perceptibly surprised. This past February, Cuba committee chair, **Jim Meyer**, and I were privileged to lead a delegation of twenty-two lawyers from the International Law Section on a three-day people-to-people visit to Havana, Cuba. Many of us have lived in Florida for decades, and approximately 80% of our group was of Cuban-American origin. Yet it was still startling to be reminded that this island nation—seemingly generations away—is, in fact, so very close to Miami.

Of course, Cuba is always a topic that evokes strong emotions, especially here in South Florida. As someone whose wife had her family's property stolen by the government, and whose close relatives were beaten and tortured by the communist Castro regime, I know the concerns. And so does the International Law Section. We are proud that the ILS has a strong and long legacy of strenuously advocating for human rights in Cuba, which we will continue to do.

Our section has met with, sponsored, and given well-publicized awards and financial stipends to Cuban dissidents. We even funded a Cuban lawyer so he could leave the country in order to study and practice in the United States. And we have published many articles in this very journal about the continuing problems with Cuba under its one-party, communist rule.

In short, we are keenly aware of the sensibilities of many in the Cuban-American community who are justifiably outraged by almost sixty years of communist oppression. We as a section believe, however, that it is not our purpose simply to oppose bad regimes; we have a duty to understand international law, whatever it is, and to educate our constituents so they can practice more effectively. This responsibility, we believe, is even greater as to Cuba, given our section's natural geographic, historic, and cultural proximity. This was the goal and purpose of our trip. And for me, it was remarkable.

Havana, whose harbor anchored the Spanish Armada over 500 years ago, could and should be one of the



A. LINDSAY

world's most beautiful cities—the Paris of the Caribbean. Regrettably, however, so many of the stunning and historic architectural façades are literally crumbling into the salt water. The problem, it seems, with taking private property is that you must then maintain it.

Folks in dark alleys greet you with a smile, don't ask for money, and only appear interested in learning about you, and what you think of their country. The locals repeatedly impress with their curiosity, and never for a minute did any of us fear for our safety. Of course, we are told that it is because this government, which had no problem stealing its citizens' land and businesses,

will exercise a strong brand of corporal punishment against anyone who steals from its tourists.

But there are currents of change on both sides of the Straits of Florida, and they are of the very type about which the section's members are interested and expected to know. In the past two years, the United States has reopened its embassy, shuttered since 1962, and remarkably, the Stars and Stripes flies again over Havana's famous Malecón. Cuba itself has made some small but important concessions to capitalism. There is now a list of 203 businesses that Cubans can own and run privately. Hair shops and bakeries are on the list; pharmaceuticals, tourism, and weapons manufacturing are not. But the *paladares*, or private restaurants, are the most visible to foreign tourists, and we made sure to support and patronize those establishments at every opportunity.

Similarly, limited but private ownership of real estate is starting to be permitted by the government. Cuban citizens are also allowed to travel internationally, and do so far more frequently than we might imagine. While censorship and government control are still a problem, we were told that there is now more Internet access than ever. Indeed, it is not uncommon to see groups of Cubans huddled around Internet hotspots, or standing outside hotels trying to get a bar or two of connectivity.

So, there is change, but as much as Cuba might seem

Message From the Chair, continued

to an American businessperson like the land of opportunity, all that glitters is certainly not gold. Anyone who doubts that Cuba remains under hard-core communist rule, even with increased foreign direct investment, need only turn the next corner to see propaganda posters, books, and even whole buildings prominently featuring the slogans and images of Che, Fidel, Raúl, and others from what feels like the bygone era of the Iron Curtain.

As the lights flickered on and off because of power outages, a political officer who spoke with us at the U.S. Embassy made clear that the Cuban government has three priorities: political control through the one-party system; a centralized economy; and social/income equality. Of course, no government in the history of humanity has ever succeeded at all three of these goals. China, for example, has incredible wealth disparity at the moment. Nonetheless, the Cuban government continues to think it is exceptional.

One of the country's largest problems, however, is that its current youth—now three generations away from the revolution and frankly, not interested—are leaving the island in droves. The lack of a young working class will soon create an unsustainable situation for Cuba's aging population. Cuba, therefore, must continue to change if it is going to survive.

We can hope that the change will be in the form of greater human rights, increased transparency, and greater personal liberty. We can perhaps also hope that the United States' rapprochement with Cuba might continue under the new U.S. administration. But we should probably expect that any change will not be fast, nor will it lead to the unbridled foreign-driven capitalism accused of predicating previous revolutions.

Whatever happens, the International Law Section, through its Cuba committee and publications like the *International Law Quarterly*, will continue to be a global leader in fairly observing and reporting on the situation.

With this, my swansong as chair of the section, I would just add that it has been a privilege and pleasure serving our membership this past year. We have an incredibly talented group of members, committee chairs, executive committee members, and board members who work every day to keep the section a global leader in information, innovation, and insight.

Safe travels,

Al Lindsay
Chair

International Law Section of The Florida Bar



Alvin Lindsay, ILS chairman (at far right), at the Hotel Nacional with Margaret Spicer, Derek González, Dennis González, Daisy González, Marco D. Britt, and Matthew D. Hinds



Alvin Lindsay, ILS chairman (at left, fourth from bottom), at dinner with his fellow travelers in Havana, Cuba



José Valdivia and Alvin Lindsay at the José Martí Memorial

International Law Section People to People Trip to Havana, Cuba 26 February – 1 March 2017

From 26 February to 1 March 2017, the International Law Section of The Florida Bar attended an educational, law-oriented, people-to-people exchange in Havana, Cuba. Participants followed a rigorous three-day schedule filled with lectures and cultural events, including meetings at the U.S. Embassy in Havana, discussions on the Cuban legal and economic systems, and tours of important historical sites in Havana.

Photos courtesy of Al Lindsay



Trip participants gather on the steps of the U.S. Embassy in Havana for a group photo.



Clockwise from top left: Carl Fornaris, Daisy González, Loly Sosa, and Alicia Menendez at Paladar San Cristobal, a Cuban-owned restaurant serving Cuban-Creole fare



As part of the cultural exchange, the group attends a performance by the Orchestra Sinfónica Juvenil, led by Director José Antonio Méndez.

People to People Trip to Havana, Cuba, continued



A live band plays as the group tours La Fábrica de Arte Cubano, a repurposed oil factory hosting art viewing, performances, and exhibitions of cinema, theater, dance, music, literature, fashion, architecture, graphic design, photography, and the visual arts.



The University of Havana



Bronze statue of José María López Lledín, known as El Caballero de París, a well-known and well-loved beggar who frequented the streets of Havana in the 1950's



The Havana cityscape at night



The historic Hotel Nacional de Cuba, which dates to 1930



Statue of Carlos Manuel de Céspedes del Castillo, leader of the first Cuban attempt to achieve independence from Spain and to free all slaves

People to People Trip to Havana, Cuba, continued



The group engages in a lunch discussion regarding Cuba's economic future.



Vintage cars in the decorative fishing town of Jaimanitas



A view of the bay from Paladar Río Mar, located at La Puntilla in Miramar



Bruno Ciuffetelli and Loly Sosa attend a lecture in Miramar.



The group is introduced to *paladares*, restaurants owned by Cuban entrepreneurs, including Paladar Río Mar, located in Miramar.

From the Editors . . .

It all started with a Saturday afternoon phone call from Sony Corporation. I was having lunch with my mother, and the Sony representative asked whether my mother was enjoying the \$17,000 worth of Sony products delivered to her home in Homestead, Florida. My mother lives in North Miami—and she had not purchased any Sony products. By the time we realized what had happened,

multiple purchases had been made with my mother's credit cards and funds had been stolen from her bank accounts. Many of our readers have similar, if not more harrowing, stories.

So, if I was already concerned with cybersecurity and

data privacy prior to reading the submissions for this Spring 2017 *International Law Quarterly: Focus on the International Aspects of Cybersecurity and Data Privacy*, the predominant feeling I have now is closer to fear.

Data rules our lives and our clients' businesses and, notwithstanding our best efforts at self-delusion, the reality is that our and our clients' sensitive, confidential business information is at risk. One need only read the headlines from our nation's newspapers to know that data privacy and cybersecurity are top-of-mind issues for our clients. We are not providing adequate legal services to our clients if we cannot counsel them on these important issues.

Luckily for our readers, this *ILQ* will bring you up to speed on some of the most salient topics in the fields of cybersecurity and data privacy.



EDITORS JAVIER PERAL, RAFAEL RIBEIRO AND LOLY SOSA



If data is stored in servers located outside of the United States, can the U.S. government obtain access to it as part of an investigation?

Bret S. Cohen, Lillian S. Hardy, and Charlie Wood start us off with an in-depth discussion

of recent case law regarding the U.S. government's ability to access data located abroad in the context of cross-border investigations.

Your client has been hacked and wants to strike back, not only to recapture the stolen information, but also to punish the hacker. Instruct them to take a breath. **Alan Brill** and **Jason Smolanoff** give us insight into the pitfalls of attempting to "hack back."

In a discussion that is sure to engage our readers who represent multinational clients, **Lillian Chaves Moon** and **Gail Gottehrer** summarize the impact of international data privacy and protection laws on an employer's ability to monitor its employees' communications while they are working outside of the United States. Continuing in the employment context, **Joseph T. King** provides guidance on how employers can protect themselves

From the Editors, continued

from former employees who “haccess” their former employers for personal gain.

Readers representing clients operating in the European Union also will do well to carefully read **Philip R. Stein’s** summary of the EU’s recent attempt to regulate data protection through the European General Protection Regulation, which will go into effect in the EU on 25 May 2018.

You have heard of the “Internet of Things,” right? What about the “Internet of Container Ships”? **Ryon L. Little** provides us with an in-depth discussion of cybersecurity issues on the high seas, including issues relating to the preservation of voyage data recorders and automatic information systems, and previews the factors that our clients will need to consider once the maritime industry begins operating autonomous vessels.

Returning to the topic of law enforcement and data privacy, **Armando Rosquete** guides us through the interplay between Mutual Legal Assistance Treaties and search warrants. **Thiago Luis Santos Sombra** presents us with a more philosophical discussion of the decline of “cyberlibertarianism” and the rise of “cyberpaternalism” and “network communitarianism,” two theoretical points of view on cyberspace. To round out our “Focus On” portion of the *ILQ*, **Peter Quinter** discusses the interplay between U.S. government trusted traveler programs such as Global Entry and issues relating to data privacy.

In the second part of our *ILQ*, our contributors tackle issues that have become even more high-profile and important after the 2016 elections and the advent of the Trump presidency.

Mariana R. Ribeiro and **Beatriz E. Osorio** present us with a detailed discussion of the factors that U.S. employers must consider with regard to the issue of employment-

based immigration in the era of Trump. **Larry S. Rifkin** builds upon that discussion and provides us with insight into how our clients should navigate I-9 audits and E-Verify procedures.

Continuing on the immigration front, but from a different angle, **Jeffrey C. Schneider** and **Marcelo Diaz-Cortes** give us an overview of the possibilities—and perils—that every EB-5 investor should consider prior to participating in the program.

Benjamin R. Rosenberg concludes the features section of our *ILQ* with a discussion of the brave new world of medical marijuana, and gives us insight into the myriad international and domestic laws that impact this burgeoning yet controversial industry.

And finally, our **World Round-Up** contributors, as usual, have not disappointed, and have provided our readers with timely and concise summaries of the most recent developments in international law in Asia, the Middle East, North America, Russia, and South America.

To the extent that it has not stressed you out and caused you to change and encrypt all of your passwords, we hope you have enjoyed our spring 2017 *International Law Quarterly: Focus on the International Aspects of Cybersecurity and Data Privacy*.

For our summer 2017 *ILQ*, we again will be focusing on a topic that is near and dear to many of our readers: international litigation and arbitration. We look forward to receiving your submissions, and we thank you again for your readership.

Sincerely,

Rafael R. Ribeiro – Editor-in-Chief

Javier Peral – Editor

Loly Sosa – Editor

**24/7 Online &
Downloadable CLE**



FloridaBarCLE

For the Bar. By the Bar.

www.floridabar.org/CLE

Access Wars: How the Second Circuit's Opinion in *Microsoft v. United States* Changes the Rules for Government Access to Data in Cross-Border Investigations

By Bret S. Cohen, Lillian S. Hardy, and Charlie Wood, Washington, D.C.

“Location, location, location.” A phrase often used to describe the value of real estate may take on a new meaning after a key 2016 decision out of the U.S. Court of Appeals for the Second Circuit weighed in on when and how the U.S. government can compel a cloud computing service provider to produce data stored abroad.

In *Microsoft v. United States*, the Second Circuit issued a setback to U.S. law enforcement authorities (and a boost for individual privacy) by ruling that search warrants for the contents of digital communications issued to certain providers of online services under the U.S. Stored Communications Act (SCA) cannot compel the production of content stored on servers outside of the United States.¹ This decision, if it stands and is applied beyond the Second Circuit (which covers Connecticut, New York, and Vermont), will have significant ramifications for U.S. law enforcement and criminal justice, as the use of online cloud computing services offering digital communication services has proliferated in recent years, and these services have become a staple source of evidence in U.S. criminal investigations involving both individuals and corporate parties.



Adding to the complexity, as the Department of Justice has continued to pursue appeals in *Microsoft*, lower courts in at least two other circuits have disagreed with the ruling. Without a unified standard, companies now confront multiple standards

governing how to comply with government-initiated requests for company data while also considering their compliance with regulations governing the production of stored data imposed by other countries in which they operate. This article provides a practical examination of these recent developments and suggestions for how companies should react to these changes.

The Stored Communications Act

The SCA was enacted as part of the Electronic Communications Privacy Act of 1986 in part to extend to electronic communications protections analogous to those provided by the Fourth Amendment. In the decade before, the Supreme Court had established the so-called “third-party doctrine,” under which it held that citizens do not have a reasonable expectation of privacy, and consequently no Fourth Amendment protections for information they voluntarily provide to third parties, including communications service providers.² In passing

Access Wars, continued

the SCA, Congress by statute imposed procedural requirements on law enforcement where, under the third-party doctrine, the Fourth Amendment imposed no restrictions.

Relevant to this discussion, the SCA prohibits “electronic communication services” and “remote computing services”—the 1986 terms referring to what we would call now online or cloud service providers—from disclosing information about their customers to the government unless the government complies with statutory requirements.³ The SCA requires different standards of proof depending on the information sought. For example, to access certain contents of electronic communications, the government must obtain a search warrant supported by probable cause⁴ while to access less sensitive non-content records, the government may issue a subpoena or obtain an SCA court order, both of which require a lower showing.⁵

Notably, a warrant issued under the SCA is not executed in the same way as a traditional warrant, by law enforcement on the premises. Rather, like a subpoena, it is served on the service provider, which then produces the information to law enforcement.⁶ Or, as in the cases

discussed below, the service provider can challenge the warrant in court.

Microsoft v. United States

In *Microsoft*, the U.S. government served an SCA warrant on Microsoft in the United States (Microsoft U.S.) seeking, among other things, the contents of emails held by Microsoft about a particular account holder.⁷ Microsoft challenged the production of the emails, arguing that because the SCA did not apply extraterritorially and emails requested by the warrant were stored on Microsoft’s servers in Ireland, it could not be compelled to produce them in response to the warrant.⁸

The district court judge held, and the U.S. government argued to the Second Circuit, that since the court had undisputed jurisdiction over Microsoft U.S., the U.S. government could compel Microsoft U.S. to produce all customer documents to which Microsoft U.S. had access, including the emails in question.⁹ The government analogized SCA warrants to subpoenas rather than search warrants because they do not involve collection

... continued on page 55



THE FLORIDA BAR
INTERNATIONAL LAW SECTION

Aballí Milne Kalil

C O U N S E L L O R S A T L A W

Aballí Milne Kalil, P.A. is a Miami legal boutique, now in its twenty-third year, which focuses its practice on international commercial litigation, international business transactions, tax and estate planning, and domestic real estate transactions. The firm’s attorneys are fluent in a number of languages including English, Spanish, Portuguese and French, and have connections with a strong network of capable lawyers across the United States, Europe, Latin America and the Far East.

www.aballi.com

When You Have Suffered a Data Breach, Attribution May Be Useful, But Hacking Back? Not So Much!

By Alan Brill, New York, and Jason Smolanoff, Los Angeles

It is a rare day when you don't see a story in the media about data breaches. Whether it involves purported hacking of political parties, theft of trade secrets, or compromise of massive numbers of customer records or credit card numbers, data breaches are in the news.

Many organizations use the security theory "assumption of breach," meaning an attacker will eventually penetrate a network. To this end, it may well be impossible to absolutely protect an organization against all data breach risks (including deliberate actions by insiders, system architecture errors that insufficiently isolate sensitive information from other data, and incidents related to outside organizations with which data is shared or by whom data is processed). For this reason, while not abandoning perimeter defenses, prudent organizations in both the public and private sectors have added system monitoring to their tool set of defensive measures. Rapid detection of an incident provides an opportunity to limit losses and to reduce the time that hackers/thieves have to exploit access they may have gained into a network. With this said, a sophisticated information security strategy is defined by an organization's ability to detect rapidly and to respond effectively to all types of incidents.

Our work involves assisting companies both to defend their network against attack and to respond effectively



once an intrusion is detected. Because of this, we get to see hundreds of actual incidents and gain insights that can be difficult to glean from the (hopefully) rare incident that will hit any individual organization.

We've learned that common questions that executives immediately ask when there is indication of a breach include the following:

- What happened? Did we actually lose data? If so, what did we lose?
- When did this happen? Is it over? Do we know for certain that it isn't a continuing incident?
- Who did it?
- What can we do to get our data back, or at least disable or destroy the perpetrator's ability to attack us?

Each one of these is a reasonable question, but immediately taking steps to implement everything

Hacking Back, continued

suggested by these questions may not be the best plan of action.

Certainly, undertaking the forensic analyses and investigative steps needed to understand in detail how a breach event happened and to create an accurate timeline of events is extremely important. Without that information, understanding the event and the data that may have been compromised will be impossible. It's the last two questions that require a bit more thought before embarking on an investigation.

Who Did It?

The question of attribution is one that, while natural to ask, should not automatically become the objective of investigative efforts.

Unfortunately, the realities of Internet investigations more often than not make it impossible to identify definitively the perpetrators of an incident. The ability to bounce communications through multiple computers in multiple countries, most of which are compromised devices operated by third parties who likely do not know that hackers have taken control of one of their machines, makes attribution difficult at best.

Other than a desire on the part of management "just to know who did this to us," there can be reasons for pursuing—at least to a reasonable degree—indicators of who carried out the breach. One of the questions that frequently come up goes to the intentions of the hackers. Do they intend to sell consumer data to other criminals to exploit in credit card frauds or identity thefts? In the United States, for example, the ability of victims to sue successfully for damages when a breach has occurred was considered by the U.S. Supreme Court in *Spokeo, Inc. v. Robins*,¹ decided on 16 May 2016, in which the Court quoted from a decision in the *Lujan* case. The Supreme Court held that "As relevant here, the injury-in-fact requirement requires a plaintiff to show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"² The need to understand the motivation of the attacker can

sometimes be gleaned from the actor to whom the breach is attributed. While attribution is not perfect, the way in which the "bad guys" performed the attack and in some cases the Internet addresses they use may provide at least an indication as to whether the perpetrators are cybercriminals or are more likely to be nation-state actors, such as a national intelligence service conducting cyberespionage operations.

Let us assume there are two breaches. In both incidents, significant amounts of nonpublic data were stolen, including personally identifiable information (PII) about employees and customers, as well as trade secrets and confidential customer information. In one case, analysis of the modus operandi of the attack and the Internet addresses implicated lead to the conclusion that the perpetrators are cybercriminals. In this case, experience tells us that their objective is likely to be economic. That is, they are likely either to use the information for crimes like identity theft, theft from consumer bank accounts, or misuse of payment cards or to sell the information on the "dark web" to other criminals who will exploit the consumer data. In the other case, the attack is attributed to nation-state actors. Our experience teaches that they are likely looking for nonpublic information that can help them meet their goals for espionage. They are less likely to sell or misuse individual data on a wide scale. They want to fly as far below the radar as possible.

Given these findings, we may be able to say that the victims of the cybercriminal's attack are more likely to suffer actual individual damage than those whose information was taken by nation-state intelligence service actions.

There are other cases in which spending time and money on attribution may not be cost effective. In those countries where commercial insurance covering data breaches is available and the victim is a policy holder, the terms of the policy will often give the insurer influence over how an investigation is conducted, and even who will conduct it. Most insurers have panels of prequalified experts that the insurer prefers to use for

... continued on page 61

Duty Free? The Effect of International Data Privacy and Protection Laws on Employers' Ability to Monitor Business Emails of Employees Working Outside the United States

By Lillian Chaves Moon, Orlando, and Gail Gottehrer, New York

In response to a technology-driven, globalized labor market, U.S. employers are increasingly branching out into other countries by having their employees travel outside the United States for extended business trips or stationing them on long-term assignments either with a corporate affiliate or as telecommuting employees. U.S. companies are also hiring telecommuting employees who are citizens of, and live in, other countries. It is critical for U.S. companies to recognize that the extensive rights they have under U.S. laws to monitor an employee's business emails do not necessarily translate to a similar entitlement when that employee is working in countries outside the United States.

While the employee's duty to follow corporate policies accompanies him on his business travels outside the United States, the employer's right to monitor that

employee's business emails does not necessarily cross the border with the employee. With each stop on the employee's international itinerary, the company's data-related rights and obligations change. Accordingly, when monitoring business emails and launching investigations using emails generated by an employee who is working outside of the United States, employers cannot reflexively apply their U.S. practices, and must evaluate the impact of the data privacy and protection laws of the other countries on their practices.

The U.S. Approach to Employee Email Monitoring

U.S. privacy laws are composed of a patchwork of state and federal laws that aim to protect the confidential nature and unauthorized disclosure of personally identifiable information (e.g., social security numbers,

dates of birth, credit card numbers, and financial account numbers) and protected health information, largely in an effort to prevent identity theft. In the employee monitoring context, employers are able to monitor employees' email activity during work hours on employer-owned equipment. Even where an employee has saved personal information on an employer-owned



International Data Privacy, continued

computer system, U.S. law generally allows an employer free reign to access the employee’s personal information that is archived in the employer’s computer systems. This is because, under U.S. law, employees do not have a reasonable expectation of privacy when using employer-owned technology. To ensure that employees understand this, U.S. employers provide them with broad electronic communications policies that advise employees that they have no reasonable expectation of privacy when utilizing company-owned equipment and that anything generated, saved, or viewed on the employer-owned system will be subject to monitoring.

Some states in the United States take a different approach, however, when the monitoring is simultaneous to the communication, such as the monitoring of an employee’s instant messaging conversations in real time. Certain states view this as being analogous to eavesdrop recording a telephone conversation, and prohibit employers from intercepting such communications under the state’s wiretap law.¹

When that instant message is saved and maintained in the employer’s computer system as part of its ordinary archiving process, however, it is not an interception and the employer may access and review it after it is saved. With the exception of attorney-client privileged emails, U.S. law does not currently make a distinction between personal information and purely business communications generated or saved by an employee on the employer-owned equipment.² Thus, if an employee saves personal communications on an employer-owned computer, tablet, phone, or laptop, the employer can access it at any time without providing the employee with advance notice or obtaining his informed consent. When the employee performs work for an employer outside of the United States, however, the legal right of the employer to access its employee’s emails can change.

... continued on page 64



**NO
INSTITUTION
BECOMES A
LEADER
WITHOUT A
GOOD REASON**

OVER
35 YEARS
OF EXPERIENCE

**FIRST
ARBITRATION
CENTER IN
BRAZIL**



**FULL MANAGEMENT CONDUCTED
BY QUALIFIED CASE MANAGERS**

ISO 9001 CERTIFIED

www.ccbc.org.br
centroarbitragem@ccbc.org.br
+55 11 4058 0400
São Paulo . SP . Brazil

Protecting Corporate Trade Secrets From Former Employee ‘Haccess’

By Joseph T. King, Tampa



Global companies must safeguard confidential, proprietary information and trade secrets—not just from cybercriminals, “hacktivists,” cyberterrorists, and competitors—but from former employees. Too often, terminated or disgruntled employees seek to extract vital information from a corporation for personal gain.

The 2017 Data Threat Report from Thales highlighted trends in data encryption and protection finding that 63% of those global respondents surveyed admit that their organizations deploy new information technologies (i.e., cloud, big data, the Internet of Things, container technology, etc.) prior to having appropriate data security measures in place.¹ According to the Thales Report, the most dangerous insiders are privileged users of data, followed by executive management.²

Assuming a breach occurs, what legal action may a company take against a former employee who hacks into a corporate database, drive, or cloud information system? What prophylactic policies and procedures must be in place to ensure database protection? How will international companies continue to secure and protect confidential information of clients and constituents in a global wireless economy? A few illustrations may offer solutions.

Launch Against a Breach

Take for example, the allegations of Estes Forwarding Worldwide, LLC (Worldwide), a Virginia limited liability company, learning from Google that a former, terminated employee from its San Francisco location

Protecting Corporate Trade Secrets, continued

accessed and downloaded Worldwide's trade secrets from his home in the state of Washington.³ Worldwide expended significant resources over several years of business compiling corporate spreadsheets detailing specific vendors used by Worldwide to pick up a shipment for delivery to the airport, transport the shipment from airport to airport, and then transport the shipment from the airport to a delivery address.⁴

According to the complaint, these compilation spreadsheets included contacts, costs, and other data accumulated over years of decisions by numerous Worldwide employees selecting global transportation solutions containing the best routing decisions, vendor costs, vendor selection, and transit times.⁵ Apparently, one year after his termination and while working for a competitor, the former employee utilized the Internet to access a Google Drive account of Worldwide, downloading the trade secrets before removing Worldwide's recovery phone number and secondary email address on file with Google Drive.⁶ The former employee changed the password to the account and created an archive. One month later, he accessed that archive and purportedly downloaded more than 1,900 spreadsheets from various employees of Worldwide that detailed the best transit solutions.⁷

Deploy the Defend Trade Secrets Act of 2016 With International Jurisdictional Reach

Worldwide sued in federal court claiming, among other things, breach of contract (in violation of employment agreements), violations of the Computer Fraud and Abuse Act (CFAA), violations of the Defend Trade Secrets Act (DTSA), unlawful access to stored communications in violation of the Stored Communications Act (SCA), and misappropriation of trade secrets, and requested a preliminary and permanent injunction.⁸

Enter the DTSA

Signed into law on 11 May 2016 as an amendment of the Economic Espionage Act of 1996, the DTSA provides civil remedies to a criminal penal statute for trade secret misappropriation. By its enactment, the "owner of a

trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."⁹

Original Jurisdiction

Thus, an international or global company may file in the United States federal district courts for misappropriation of trade secrets so long as the company intends to use, or uses, the product or service in foreign commerce. This is a key component to the DTSA that opens the door to civil seizure orders by international companies trying to thwart corporate espionage of intellectual property overseas.¹⁰

The DTSA affords original jurisdiction with United States federal district courts for a claim of trade secret misappropriation.¹¹ Federal courts may grant injunctive relief and prevent actual or threatened misappropriation by issuance of an order seizing property upon ex parte application, but only in extraordinary circumstances.¹²

Civil Seizure

Prior to its enactment, companies seeking redress for trade secret misappropriation had no choice but to sue in state court, utilizing varying statutory laws of the different states.¹³ Under extraordinary circumstances, by employing the DTSA, a company aware of a potential misappropriation of its trade secrets may file an ex parte application seeking an "order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."¹⁴ In short, companies may file for ex parte relief to seize a server, a computer, a flash drive, or a cell phone utilized to misappropriate trade secrets.

Limitations

The DTSA maintains a three-year statute of limitations beginning when the company knew or should have known through the exercise of reasonable due diligence of the theft.¹⁵ Notably, a "continuing misappropriation"

... continued on page 73

The EU's Attempt at a Comprehensive Approach to Regulation and Enforcement of Data Protection

By Philip R. Stein, Miami

In recent years, the United States has been roiled by one instance after another of high-profile, large-scale breaches of data security. The list of such episodes include a foreign power's access of politically sensitive Democratic Party

emails during the 2016 election cycle, two huge breaches of Yahoo! user account data, and the hacking of the personally identifiable information (PII) of customers of major retailers Target and The Home Depot, among many others. Yet the legislative and regulatory response in the United States to the exponentially growing problem of data privacy violations has been largely muted, or at least far from uniform or systematic. A plethora of governmental agencies—such as the Department of Justice, the Federal Trade Commission, and the Securities and Exchange Commission—have made clear that each understands data protection issues as being within its respective purviews. But a compliance officer looking for comprehensive, non-agency-specific guidance as to what a company must do to protect PII and other sensitive data in the United States is not likely to be satisfied. Perhaps even more importantly, as a general matter, a U.S. citizen can point to little that is definitive, let alone uniform, across various industries and contexts regarding how (and to what extent) her PII will be safeguarded.

By contrast, the European Union (EU) has in recent years



manifested a clear intention to maximize protection of personal data, and has sought to do so in a reasonably comprehensive and ascertainable manner. A particularly noteworthy product of that intention is the new

European General Data Protection Regulation (GDPR), which will come into force throughout the EU on 25 May 2018. The GDPR will replace existing data protection laws throughout the EU and will introduce significant changes and additional requirements that will have a wide-ranging impact on individual rights, business requirements, and the police and criminal justice sectors. This article offers an overview of the history and key components of the GDPR, and some comments on how it might fare as an attempt to stem the rising tide of cyberbreaches.

History

EU legislation on data protection has been in place since 1995. The core aspect of that legislation has been a Data Protection Directive (formally, Directive 95/46/EC) that guarantees effective data protection. The right to such protection is deemed fundamental in the EU pursuant to Article 8 of the EU's Charter of Fundamental Rights; however, each member state has, to some meaningful extent, implemented the law differently. Consequently,

Data Protection in the EU, continued

there has been uncertainty as to how the law should be interpreted and applied, as well as higher-than-desirable costs associated with administering the law.

Moreover, in recent years there has been growing recognition that the EU's data protection rules need to be updated in any event. Processing of personal data has grown exponentially since 1995, with the proliferation of digital media, cloud computing, and location-based technology. The EU perceived that a more modernized, robust set of regulations would afford greater protections at a time when they were sorely needed and could also serve as a boon to the development of the digital economy within its borders.

In December 2015, an arduous process of agreeing to specific reform legislation was completed. Ratification of the new legislation occurred in early 2016. There are two major components of the reform:

The General Data Protection Regulation (GDPR), which is designed to enable individuals to better control their personal data. The GDPR reflects the EU's hope that

modernized and unified rules will permit businesses to derive maximum benefit from the opportunities of a contemplated "Digital Single Market," by reducing regulation and benefiting from enhanced consumer trust that personal data will be protected.

The Data Protection Directive, which requires the police and criminal justice sectors to ensure that the data of victims, witnesses, and suspects of crimes are appropriately protected in the context of a criminal investigation or a law enforcement action. More harmonized laws across member states will also facilitate better cross-border cooperation of police or prosecutors in their efforts to combat crime and terrorism more effectively across Europe.

Member states have now completed roughly one-half of a two-year implementation period. A clearer view is now emerging of various practical implications of the two aforementioned components of the new legislation:

... continued on page 77

Global reach. Local roots.

Hogan Lovells' International Arbitration practice brings extensive experience to the resolution of complex, high-value international business disputes through commercial or investment treaty arbitration.

With access to the most sophisticated technology, our multilingual and multicultural lawyers operate from a network of offices in all major dispute centers and have a footprint in the world's emerging markets. Whether down the street or across the world, our lawyers bring global experience with local market knowledge.

Daniel E. González
Global Head, International Arbitration
Miami, T +1 305 459 6649
daniel.gonzalez@hoganlovells.com

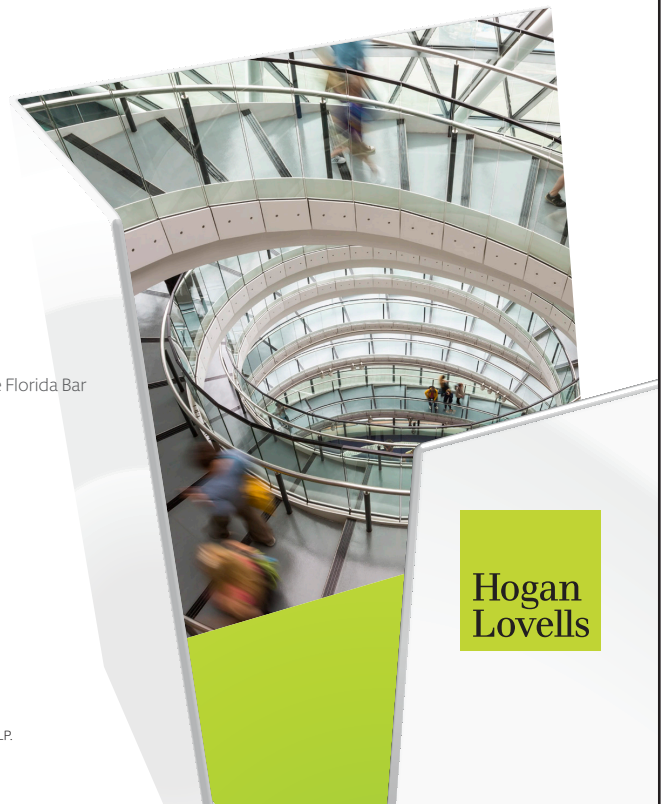
Mark R. Cheskin, Partner
Miami, T +1 305 459 6625
mark.cheskin@hoganlovells.com

Alvin F. Lindsay, Partner
Chair, International Law Section, The Florida Bar
Miami, T +1 305 459 6633
alvin.lindsay@hoganlovells.com

Richard C. Lorenzo, Partner
Miami, T +1 305 459 6652
richard.lorenzo@hoganlovells.com

2,500+ lawyers. 45+ offices. 25 countries.
hoganlovells.com

Hogan Lovells is an international legal practice that includes Hogan Lovells US LLP and Hogan Lovells International LLP.
© Hogan Lovells 2016. All rights reserved.



**Hogan
Lovells**

Cybersecurity: A Sea Change in Maritime Commerce

By Ryon L. Little, Miami

“The harsh reality of 21st century military cyber activity is that the heavy reliance on civilian products and infrastructure dramatically expands the universe of targetable objects, including systems on which important civilian functions rely.”¹

Today’s merchant vessels include container ships, bulk cargo ships, and tankers that together transport 90% of the world’s goods.² The shipboard technology used by the maritime industry to facilitate the worldwide transportation of goods and commodities is

interconnected

and vulnerable

to cyberattack.

Indeed, as

international

supply chains

have evolved into

a “just-in-time”

inventory model,³

the efficiencies

created also open

up consumers,

stores, and nations

that rely on timely

stocked shelves to

vulnerabilities and

disruptions due

to interruptions

in the maritime

transportation system. It is hard to imagine a more important civilian function than ensuring food and other necessary goods are safely and timely transported to a nation’s population centers. Corporations involved in international maritime commerce continue to embrace and leverage technology in order to improve efficiency and to reduce the cost of ocean transport of goods and raw materials. The computer software and hardware employed in maritime commerce mirror the data-driven technologies being used to streamline and document nearly every facet of commercial enterprise. Reliance on technology in the maritime industry requires that

ship owners, ship charterers, and marine insurers make adequate preparations to ensure that the electronic information and communication systems that underpin the maritime industry are protected from compromise by a cybersecurity event.



The Current International Framework Is Insufficient

There is an international framework in place that promotes uniformity in securing the maritime supply chain and maritime infrastructure. International conventions dealing with maritime security, such as the International Ship

and Port Facility Security (ISPS) Code, have been adopted under the auspices of the International Maritime Organization (IMO)⁴ by the contracting governments to the International Convention for the Safety of Life at Sea (SOLAS). The ISPS Code establishes baseline security requirements for contracting governments of countries where commercial ports are located and contracting governments of countries where ships are registered. Individual nations can, and often do, set higher standards for their own port facilities and for vessels documented in that country. The United States has chosen to set higher standards, largely through the Maritime

Maritime Cybersecurity, continued

Transportation Security Act of 2002 (MTSA).⁵ The MTSA was enacted as a reaction to the 11 September 2001 terrorist attacks and places a significant amount of the responsibility for coordinating maritime security efforts with the U.S. Coast Guard; however, the MTSA does not address any specific cybersecurity concerns. To the Coast Guard's credit, it has worked to promulgate regulations (found in 33 C.F.R. Parts 101 - 107) that more specifically address issues of vessel and maritime security, but the regulations only generally refer to security measures for a vessel or a company's systems and equipment.

Industry leaders and regulatory agencies have recently taken a closer look at the vulnerabilities of the distinctly maritime electronic information systems that keep maritime commerce on track. In June 2015, the U.S. Coast Guard issued its mission policy statement on cybersecurity, *United States Coast Guard – Cyber Strategy*.⁶ In the introduction to the U.S. Coast Guard – Cyber Strategy, the threat is spelled out clearly:

Our adversaries employ sophisticated tools and possess substantial resources. They include state-sponsored and independent hacker groups, terrorists, Transnational Organized Crime groups, as well as corrupt, disgruntled, and complacent employees (commonly referred to as insider threats). These growing threats also pose significant risks to our Nation's Maritime Transportation System (MTS) and critical infrastructure, and by direct extension, our Nation's security and economic stability. With approximately 360 sea and river ports, which handle more than \$1.3 trillion in annual cargo, our Nation is critically dependent on a safe, secure, and efficient MTS, which in-turn is highly dependent on a complex, globally-networked system of automated cyber technology.⁷

As it relates to the maritime industry, the U.S. Coast Guard – Cyber Strategy makes a priority the protection of maritime critical infrastructure, which includes “. . . the ports, facilities, vessels, and related systems that facilitate trade within the U.S., support national defense and homeland security objectives, and

... continued on page 82



reedsmith.com

International Law

Global firm. Local commitment.

Reed Smith is a global relationship law firm with more than 1,700 lawyers in 27 offices throughout the United States, Europe, Asia and the Middle East.

Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, entertainment and media, shipping and transport, energy and natural resources, real estate, manufacturing and technology, and education.

ReedSmith
Driving progress
through partnership

International Legal Assistance and Special Considerations Presented in the Cybercrime Context

By Armando Rosquete, Miami

Introduction

Criminal investigations are not immune from the increasing sophistication of criminal actors and their evolving use of technology. Indeed, most judges and criminal-law practitioners would readily admit to a steady rise in cybercrimes, including conduct ranging from hacking to identity-theft schemes seeking to monetize data.¹ The criminal monetization of data, such as identifying information or financial information, frequently funds other criminal endeavors. And, often, the most challenging aspects of these schemes involve the identification and collection of evidence in foreign jurisdictions.

This article discusses the various methods for facilitating cross-border cooperation in criminal matters and some unique issues presented in the cybercrime context. These include the interplay between Mutual Legal Assistance Treaties (MLATs) and search warrants, as well as the possibility that recent changes to Fed. R. Crim. P. 41's search warrant provisions for computers and electronically stored information (ESI) may support similar changes to 18 U.S.C. § 3512's current constraint on the manner in which a U.S. court addresses a foreign state's MLAT request for a Rule 41 search warrant.

Letters Rogatory

Letters rogatory are the customary method of obtaining international legal assistance in the absence of a treaty



or an executive agreement.² A letter rogatory is a request from a judge in the United States to the judiciary of a foreign country requesting testimony or other evidence, which, if done without the sanction of the foreign court, would constitute a violation of that country's sovereignty. Federal courts in the United States have the power to issue letters rogatory pursuant to 28 U.S.C. § 1781 (Transmittal of Letter Rogatory or Request) and Fed. R. Civ. P. 28(b) (Persons Before Whom Depositions May Be Taken). The U.S. Department of Justice (DOJ) views letters rogatory as a last resort and instructs its prosecutors to assume that the process will take a year or more.³ Prosecutors may potentially shorten the time if they transmit a copy of the request through Interpol or through some other more direct route. Even in urgent cases, however, letters rogatory may take over a month to execute.⁴

International Legal Assistance, continued

MLATs

In contrast to letters rogatory, MLATs are the predominant method for facilitating cross-border cooperation in the criminal context. But extradition treaties and applicable tax treaties may also contain provisions for obtaining particular types of evidence from abroad.⁵ MLATs contain binding obligations that subject discovery to constitutional restrictions. In the United States, “MLATs transform foreign requests into domestically enforceable orders” by directing those requests to the DOJ’s Office of International Affairs (OIA).⁶ OIA confirms that a particular request is properly presented and assigns it to the proper federal prosecutor, who then seeks a discovery order from a federal judge.⁷ In general, the court’s review of the government’s motion is focused on potential Fourth or Fifth Amendment violations and human-rights risks. Once the court issues a discovery order, DOJ will review any subsequent production of documents or ESI, seeking to remove any excess data and ensuring that the domestic data-privacy rights are respected.

The United States has executed MLATs with more than sixty foreign nations, using them to target a variety of crimes, including cybercrimes and related offenses that often have an inherent transnational component.⁸ The first three MLATs that the United States signed were with Switzerland, Turkey, and the Netherlands, and included provisions granting access to defense counsel.⁹ This more inclusive approach has been abandoned, and modern MLATs do not create individual rights or provide direct mechanisms for private parties, such as criminal defendants, to request the production of evidence located abroad.¹⁰ Criminal defendants are left with letters rogatory to secure such evidence—“a far less efficient and reliable process.”¹¹

18 U.S.C. § 3512: A Statute Aimed at Streamlining Foreign Requests for Assistance in Criminal Matters

18 U.S.C. § 3512 is a legal-assistance statute that is expressly limited to foreign requests for assistance in criminal matters. “Reflecting the realization that MLATs are now a well-worn tool in the prosecutors’ toolbox,

Congress passed [18 U.S.C. § 3512 as part of the “Foreign Evidence Request Efficiency Act of 2009,” Pub. L. No. 111–79, 123 Stat. 2086].¹² The act was explicitly passed to help streamline the MLAT process, making it ‘easier for the United States to respond to requests by allowing them to be centralized and by putting the process for handling them within a clear statutory system.’”¹³

Among its key advantages, Section 3512 provides for a more streamlined process than the one provided under the more well-known 28 U.S.C. § 1782,¹⁴ a similar statute that can apply in civil *and* criminal cases.¹⁵ Section 1782 has the advantage of versatility as well as a statutory language and a body of case law that is, generally speaking, friendly to the entity seeking discovery. Nonetheless, law enforcement does not typically rely on Section 1782 for a variety of reasons.¹⁶ Section 1782 when deployed in the criminal arena requires the U.S. attorney general, as the central authority, to respond to requests for evidence from foreign governments by filing Section 1782 applications with the district court in every district in which evidence or witnesses may be found. In cases where the requesting state seeks evidence located in multiple jurisdictions, Section 1782 requires the attorney general to appoint multiple federal prosecutors in the districts where the specific evidence is located.¹⁷ By contrast, Section 3512 permits a *single* federal prosecutor to pursue requests in *multiple* judicial districts.¹⁸ With the exception of search warrants, Section 3512 also allows a district court judge handling an MLAT request to oversee and approve subpoenas and other orders with effect in districts other than their own.¹⁹

The Second Circuit Reinforces the Role of MLATs in *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016)

“Particularly in the area of high-tech crime, obtaining evidence through the use of formal MLATs between nations can be time consuming. . . . In more complex

... continued on page 86

Internet Regulation and Data Protection: The Role of Law Enforcement

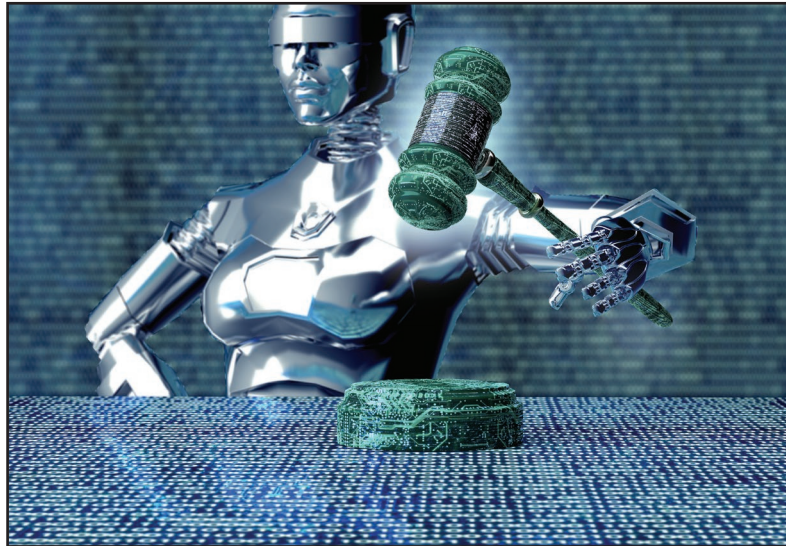
By Thiago Luís Santos Sombra, Brasília

Regulation in cyberspace is becoming a myth in some parts of the world. While prohibiting software, platforms, and services like Uber, nation states are trying to deal with the disruption and convergence issue, not understanding the aim and the benefits of regulation. This essay analyzes regulation in cyberspace as the next challenge of the general theory of law enforcement.

Regulation in Cyberspace

One of the most interesting themes encountered when undertaking research about cyberspace concerns its regulation in regard to civil society and law enforcement. One of the aims of this research is to comprehend how people's behavior in everyday life differs from their behavior in cyberspace, and what impact this difference may have on regulation.¹ This article includes a brief history of cyberlibertarianism and its decline, and then offers an explanation of cyberpaternalism and network communitarianism, two different theoretical points of view on cyberspace.

As an initial matter, regardless of which theory is most supported, it is essential to understand how intervention in cyberspace differs from regulation in real life. In this respect, a proper understanding of the particularities of cyberspace requires us to necessarily change some aspects of our conceptualization of the general theory of the law,² which has been constructed solely to resolve problems related to property, the rivalrousness of goods,



and the physical limitations of the atomic world.³ The theoretical disputes are no longer the greatest debate about legality and morality in law.⁴ Theorization of the law throughout the twentieth century has always centered on the key themes of property and possession; this was suitable when dealing with physical

goods,⁵ but is not suitable in the realm of cyberspace when dealing with information, ideas, or the sharing economy.⁶

In the past, modern economies were structured around the ownership of material things,⁷ as highlighted by John Perry Barlow.⁸ Now the law has transitioned, due to the growth of cyberspace and its key element, information, which is not based on atoms, but on bits.⁹ Thomas Jefferson was perhaps the first man who imagined how the future could be changed by information and ideas, especially in an age when people thought only about the exclusiveness of property, as we can deduce from his letter to Isaac McPherson.¹⁰

The digitization and disruption processes that society is currently undergoing show us that nonrivalrous goods will allow us to consume, share, and produce information simultaneously,¹¹ in an unlimited manner, wherever we are and for whatever reason each person consumes it.¹² Notwithstanding the above, the law should have the ability to deal with these shifts.¹³ If information is to be our principal good and our main source of wealth—the so-called oil of the twenty-first century—then perhaps the challenges will not be in terms of ownership, but in

Internet Regulation and Data Protection, continued

terms of sharing information and ideas; in other words, “bits” being transferred across the globe.¹⁴

This ongoing process will represent not a change in providers, but changes regarding the services and benefits offered in society, for law cannot regulate the content itself, so it affects the recipient as Barlow has outlined with his analogy of the wine and its bottle. Law cannot affect cyberspace directly, sanctioning the actually bytes, but it can influence the physical world that supports it.

We experience numerous examples of revolutionary services, the so-called “disruptive technologies” from Uber, Airbnb, Spotify, Coursera, Netflix, VinyLify, and Prosper Marketplace all the way to SSRN-Social Science Research. Despite these variations of “bottles,” to use Barlow’s expression, it remains unclear whether the law will be successful in taming cyberspace. Why should cyberspace be regulated, who has the legitimacy to do so, who represents whom, and how will territorial limits be

drawn?¹⁵ Will sharing instead of owning change human relationships and the way the law regulates behavior? These are the key questions that this article addresses and will seek to answer.

The Cyberlibertarians and the Discovery of Cyberspace

The so-called cyberlibertarians were the first to consider the perspective of regulating rule or behavior in cyberspace. Following the creation of the World Wide Web in 1989 by Tim Berners-Lee,¹⁶ this new tool created or influenced many outcomes, which have expanded drastically over the years. Amidst this new environment, people were dazzled by the global real-time interaction it provided. Emails, chat groups, instant information sharing, and other new services quickly sparked the interest of the public, and the debate soon ignited

... continued on page 91

Sequor Law proudly salutes The Florida Bar International Law Section and its leadership among international law organizations.

You Provide a Platform for Florida’s International Practitioners to Lead Globally with Information, Innovation and Insight.

Sequor Law will continue to support your efforts as we represent clients worldwide with investigations, asset recovery and financial fraud matters, cross-border insolvencies, and commercial and financial services litigation.



SEQUOR LAW

Relentless. Global. Pursuit.
www.SequorLaw.com

Homeland Security and Data Privacy: A Primer on Customs' Global Entry Program

By Peter Quinter, Miami



clearance for preapproved, low-risk travelers upon arrival in the United States. At airports, program members proceed to Global Entry kiosks, present their machine-readable passport or U.S. permanent resident card, place their fingerprints on the scanner for fingerprint verification, and complete a customs declaration. The kiosk issues the traveler a transaction receipt and directs the traveler to baggage claim and the exit.

Global Entry members are eligible to participate

The U.S. Department of Homeland Security and particularly its U.S. Customs and Border Protection (CBP) have a “Trusted Traveler” program called “Global Entry.” See GlobalEntry.gov. Most likely, as international lawyers, many of us are already members of Global Entry, and receive expedited international traveler clearance by CBP upon arrival to the United States. Plus, we get the extra advantage of automatic membership in TSA Pre✓®. There are now more than two million members in the Global Entry program.

Unfortunately, the reality for many applicants to Global Entry is that their applications are denied, and current members can have their membership revoked by CBP for one reason or another. This article will describe eligibility requirements for membership in Global Entry, the benefits of membership in Global Entry, how to apply for membership, and, importantly, how you can challenge any denial or revocation of membership with CBP.

Global Entry is a CBP program that allows expedited

in TSA Pre✓. U.S. citizens and U.S. lawful permanent residents enrolled in NEXUS or SENTRI are also eligible to participate in TSA Pre✓, as are Canadian citizens who are members of NEXUS. A Global Entry member or eligible NEXUS or SENTRI member may enter his or her membership number (PASS ID) in the “Known Traveler Number” field when booking airline reservations. Better yet, enter your PASS ID into your frequent flyer profile with the airline. The membership number enables Transportation Security Administration’s (TSA) Secure Flight System to verify that you are a legitimate CBP Trusted Traveler and eligible to participate in TSA Pre✓.

Global Entry is CBP’s most popular Trusted Traveler program. But not everyone is eligible. U.S. citizens, U.S. lawful permanent residents, and citizens of the following countries are eligible for Global Entry membership: Colombia, United Kingdom, Germany, Panama, Singapore, South Korea, and Mexico. Canadian citizens and residents are eligible for Global Entry benefits

Customs' Global Entry Program, continued

through membership in the NEXUS program. Please note that applicants under the age of 18 must have a parent's or a legal guardian's consent to participate in the program.

Travelers must be pre-approved for the Global Entry program. Global Entry is a voluntary program available to travelers who pass a comprehensive background investigation. There is a computer check against criminal, law enforcement, customs, immigration, agriculture, and terrorist indices to include biometric fingerprint checks and then a personal interview with a CBP officer. Most applicants receive a formal letter that states, in part: "We are pleased to inform you that your U.S. Customs and Border Protection (CBP) Global Entry program membership has been approved. You may use the program as soon as you receive and activate your new Global Entry card."

Many applicants never receive such a welcoming letter from CBP. An applicant may not be eligible for participation in the Global Entry program if he or she:

1. Provided false or incomplete information on the application;
2. Has been convicted of any criminal offense or has pending criminal charges or outstanding warrants (to include driving under the influence);
3. Has been found in violation of any customs, immigration, or agriculture regulations or laws in any country;
4. Is the subject of an ongoing investigation by any federal, state, or local law enforcement agency;
5. Is inadmissible to the United States under immigration regulation, including applicants with approved waivers of inadmissibility or parole documentation; or
6. Cannot satisfy CBP of his or her low-risk status.

Now you realize the benefits of membership in Global Entry and you are eligible to apply for Global Entry, so the next step is to apply. The steps are very simple.

1. Create a Global Online Enrollment System (GOES) account.
2. Log in to your GOES account and complete the application. A US\$100 nonrefundable fee is required

with each completed application.

3. After accepting your completed application and fee, CBP will review your application. If your application is conditionally approved, then your GOES account will instruct you to schedule an interview at a Global Entry Enrollment Center located at most international airports. Each applicant must schedule a separate interview.
4. You will need to bring your valid passport(s) and one other form of identification, such as a driver's license or ID card to the interview. If you are a lawful permanent resident, you must present your machine-readable permanent resident card.

In the event an applicant is denied or membership has been revoked from Global Entry or other Trusted Traveler program, the person should be provided information in writing detailing the reason for this action.

Unfortunately, the reality is that the standard statement provided to the applicant merely concludes: "You do not meet the program eligibility requirements." For members whose membership is revoked, the standard instruction from CBP is "You have been found to have violated CBP laws, regulations, or other related laws." That's it; nothing else is provided. The only appeal to such a denial or revocation is a written appeal to the CBP trusted traveler ombudsman to request reconsideration.

I have seen many applicants, including attorneys, be denied membership in Global Entry. There are a variety of reasons for such a denial, including: juvenile criminal history, immigration problems, court expunged criminal information, and questionable international travel history. Even a shoplifting or assault misdemeanor is sufficient for CBP to deny an applicant membership in Global Entry. A violation that occurred thirty or forty years ago or was committed in another country is sufficient for CBP to deny membership in Global Entry. The U.S. Department of Homeland Security has extremely extensive data available to it worldwide to determine whether someone is a low-risk international traveler who should be admitted into the Global Entry program. If you believe your data is private, when it

... continued on page 96

Feeling Pushed Up Against the Wall? Current U.S. Immigration Climate Demands That U.S. Employers ‘Think Outside the Box’

By Mariana R. Ribeiro and Beatriz E. Osorio, Miami

With fewer than seventy-five days in office at the time of this writing, President Donald J. Trump has issued four widely publicized Executive Orders on immigration. These Executive Orders¹ have compelled a pause on admission to the United States for nationals of specific countries and have heightened enforcement procedures against undocumented immigrants. While the Executive Orders

have received substantial national and international mainstream media attention, less press coverage has been devoted to the 23 January 2017 leaked draft Executive Order, titled *Executive Order on Protecting American Jobs and Workers by Strengthening the Integrity of Foreign Worker Visa Programs* and several legislative proposals introduced in the U.S. Senate and the U.S. House of Representatives, which, if passed in their present form, would result in major changes to certain nonimmigrant (temporary) employment-based visa classifications commonly used by U.S. employers to obtain critical talent. In addition to the Executive Orders’ impact, the tenor of broadened enforcement in the immigration arena has created an atmosphere of uncertainty, particularly for employers and for foreign national employees working in the United States pursuant to nonimmigrant employment-based



visa petitions. As further discussed below, the current climate and specifically, the proposed legislation, which if passed would further restrict certain commonly used temporary employment-based visa classifications (in particular the Specialty Occupation Worker H-1B and the Intracompany Transferee L-1), should incentivize U.S. employers that may require foreign national employees to meet their needs for critical talent in specific positions to “think outside the box.” Exploration of alternative visa classifications, such as the Treaty Investor E-2 and the Extraordinary Ability O-1, in conjunction with business immigration counsel is one strategy that may prove effective to fill critical employment needs.

Employment-based immigration provides the mechanism for U.S. employers to employ highly skilled, professional, and educated foreign nationals. The H-1B

Think Outside the Box, continued

visa classification is commonly used by U.S. employers in a wide range of industries, including engineering, information technology, health care, finance, and education, among others, and allows U.S. employers to petition for foreign professionals to work in “specialty occupations.”² The position must be deemed a specialty occupation based upon a series of factors, among which is that the position has a minimum entry requirement of the attainment of a baccalaureate or higher degree in a specific specialty, or its equivalent.³ As a prerequisite to the filing of an H-1B petition with the U.S. Citizenship and Immigration Service (USCIS), employers must file a Labor Condition Application (LCA) with the U.S. Department of Labor (DOL).⁴ The LCA is designed to protect American workers by ensuring that (1) employers pay H-1B workers the greater of the “actual wage” or “prevailing wage” as those terms are defined by the regulations;⁵ (2) the working conditions of the H-1B employee will not adversely affect the working conditions of similarly employed U.S. workers;⁶ (3) the H-1B employee is not being hired to replace U.S. workers during a strike, lockout, or work stoppage;⁷ and (4) notice of the filing of the LCA has been given to the employer’s U.S. workers in the same occupational classification.⁸ The L-1 classification is heavily relied upon by multinational companies to transfer executives and managers from abroad to lead their operations. The L-1 intracompany transferee classification facilitates the temporary transfer to the United States of foreign nationals to continue employment with an office of the same employer, its parent, branch, subsidiary, or affiliate in a managerial, executive, or specialized knowledge position.⁹

As discussed below, in the last several years, there has been a trend of increased scrutiny of both the H-1B and L-1 classifications by U.S. government agencies involved in their processing, due to perceptions of abuse. In light of the current administration’s stance on immigration, such trends are likely to continue, and if proposed legislation passes in its current form, employment-based visas may soon have a new set of legal standards, focused on a “merit based system.”

The Writing on the Wall: Increased Scrutiny of the H-1B and L-1 Classifications

U.S. immigration laws and policy have, during various time periods, waxed and waned with respect to their enforcement stance. Historically, such stances have been fueled by both competing interests of promoting international commerce and protecting the U.S. workforce. The most recent wave of USCIS scrutiny of the H-1B classification dates back to 2008, when the USCIS published the *H-1B Benefit Fraud and Compliance Assessment* (BFCA). The BFCA found that more than 13% of the H-1B petitions reviewed were fraudulent.¹⁰ Following publication of the results of the BFCA, several initiatives and programs were instituted by USCIS to tackle the wide-ranging perception that the H-1B classification was fraught with fraud. Specifically, one month subsequent to the BFCA’s publication, Donald Neufeld, then acting associate director for domestic operations, USCIS, issued a guidance memorandum entitled *H-1B Anti-Fraud Initiatives - Internal Guidance and Procedures in Response to Findings Revealed in H-1B Benefit Fraud and Compliance Assessment*. This guidance provided parameters for the review and referral of petitions to the USCIS’s fraud detection operations, and instructed the field to issue Requests for Additional Evidence (RFE), Notices of Intent to Deny, or Notices of Intent to Revoke in cases in which an adjudicator becomes aware of potential violations or noncompliance with the H-1B program.¹¹

Additionally, in 2009, the USCIS awarded a contract to Dun and Bradstreet to act as an independent information provider for its new program, Verification Initiative for Business Enterprises (VIBE). The VIBE program is a web-based service that uses commercially available data from an independent information provider to validate and verify information submitted by organizations that petition to employ foreign workers in the H-1B and L-1 classifications.¹² In furtherance of the USCIS’s increased scrutiny of the H-1B and L-1 classifications, in July 2009, the USCIS commenced the Administrative Site Visit and

... continued on page 98

Worksite Enforcement: An Attorney's Role in Counseling Employers About the I-9 Audit Process and E-Verify

By Larry S. Rifkin, Miami

On 26 January 2017, President Donald S. Trump signed Executive Order *Enhancing Public Safety in the Interior of the United States*

to increase immigration enforcement actions by hiring an additional 10,000 immigration officers.¹ This Executive Order is expected to increase the number of worksite enforcement audits and raids as a means of addressing the issue of an estimated eleven million immigrants living in the United States illegally.² The Trump administration has also pushed for requiring *all* employers to use E-Verify in their hiring practices.³ U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) is responsible for engaging in effective worksite enforcement. This article will examine the consequences of these enforcement actions for U.S. employers and how attorneys can help them comply with established laws and regulations in order to limit the employers' civil and criminal liability. The article will also examine the pros and cons of the E-Verify program for employers.

ICE's Objectives

Historically, U.S. Immigration and Customs Enforcement (ICE), under the Department of Homeland Security (DHS), has engaged in a "comprehensive worksite enforcement strategy that promotes national security, protects critical infrastructure and targets employers who violate employment laws or engage in abuse or exploitation of workers."⁴ According to the ICE website on worksite enforcement, the agency's goal is twofold:

1. ICE will look for evidence of the mistreatment of workers, along with evidence of trafficking, smuggling, harboring, visa fraud, identification document fraud, money laundering, and other such criminal conduct.



2. ICE will obtain indictments, criminal arrests, or search warrants, or a commitment from a U.S. Attorney's Office to prosecute the targeted employer before arresting employees for civil immigration violations at a worksite.⁵

ICE's worksite enforcement strategy includes using Form I-9 inspections, civil fines, and debarment to penalize employers and to deter illegal employment.⁶

Form I-9 Procedures

Congress passed the Immigration Reform and Control Act of 1986 (IRCA), which prohibits employers from employing individuals that they know are not authorized to work in the United States.⁷ Under IRCA, it is illegal for an employer to knowingly hire and continue to employ unauthorized workers.⁸ The Act also established criminal and civil sanctions, as well as fines for employers that do not comply with the law.⁹

Since November 1986, all U.S. employers must ensure proper completion of Form I-9, Employment Eligibility Verification, for each individual they hire for employment in the United States. This includes citizens and noncitizens.¹⁰ As of 22 January 2017, employers must use the 11/14/2016 N version of Form I-9 to verify the identity and work eligibility of every new employee hired, or for the re-verification of expiring employment authorization of current employees (if applicable).¹¹ The form itself consists of three pages with three sections and a supplemental fourth page listing acceptable identity and employment authorization documents.¹²

Worksite Enforcement, continued

Both the employee and the employer (or authorized representatives of the employer) must complete Form I-9. The employee completes section 1 (only) on or before the first day of employment; the employer must complete section 2 within three days.¹³ On section 1, an employee must attest to his or her employment authorization by marking whether he or she is a U.S. citizen, a noncitizen national of the United States, a lawful permanent resident, or an alien authorized to work until a specific date, usually tied to the expiration of his or her employment authorization document. The employee must also present the employer with acceptable documents evidencing identity and employment authorization. The employee signs the form at the bottom of page 1, under penalty of perjury, as to his or her knowledge of the penalties for false statements and false documents and his or her authorization to work.¹⁴

The employer is liable for all information provided on Form I-9. As such, the employer must examine the employment eligibility and identity document(s) an employee presents in order to determine whether the document(s) reasonably appears to be genuine and relates to the employee before recording the document information on the Form I-9.¹⁵ The employer signs the form on page 2, under penalty of perjury, that it has examined the employee's documentation and has verified the individual's ability to work lawfully in the United States.¹⁶ If the employee's employment authorization expires at some future date, the employer must re-verify such authorization on or before the expiration date of the original document.¹⁷ The employer does so by completing section 3 of the current Form I-9. Employers must retain Form I-9 for the later of three years after the employee's hire date or one year after the employee's termination date.¹⁸ The employer must also make the Form I-9 available for inspection by authorized government officers.

Form I-9 Audit Process

Form I-9 compliance inspections are initiated by field offices after receiving a tip line complaint or through

an HSI headquarters initiative.¹⁹ The inspection process begins when HSI serves a Notice of Inspection on an employer, compelling the business to produce I-9's for all current and past employees for the last three years, as well as various documents, such as a copy of the employer's payroll, articles of incorporation, and business licenses.²⁰ The Notice of Inspection will require that the documents be delivered to the HSI special agent in charge within three business days.²¹

At this point, it is important for the employer to contact an attorney, who can assist with the preparation of the submission of the requested documents and, most likely, negotiate an extension of the due date. The attorney's role in this process is to limit the employer's liability by demonstrating to the HSI special agent that the employer has made a good-faith effort to comply with Form I-9 regulations. An attorney can assist an employer's good-faith efforts to mitigate its civil and/or criminal liability, such as late completion of any Form I-9 for any active employees whose form is not located or available; work with an employer and employee(s) to correct any technical errors on Form I-9; explain the unavailability of any documents requested; and highlight factors that will support the narrative of a good-faith employer.

After HSI receives the requested documents from the employer, the agency will then inspect the Form I-9 for each employee and classify any violations as either technical or substantive, based on the seriousness of the errors or omissions. Technical violations include failing to ensure that an individual has provided all personal information on the I-9, such as a maiden name, address, and birth date.²² Substantive violations include one or more instances of an employee failing to present a Form I-9 and an employer failing to review and verify required documentation.²³ After the inspection, the employer will receive a Notice of Technical/Procedural Failures. Technical errors on I-9's will not result in civil fines if corrected within ten business days by either the employee or the employer, or both, as needed.²⁴ After ten business days, uncorrected technical and procedural failures will become substantive violations.²⁵ HSI may

Worksite Enforcement, continued



also provide the employer with a Notice of Suspect Documents, wherein the agency alerts the employer that it has determined that an employee is not authorized to work based on the I-9 information provided.²⁶ The notice advises the employer of criminal and civil penalties for continuing to employ the named individual(s). If HSI cannot determine the validity of a particular employee's work authorization, it will issue the employer a Notice of Discrepancies directing the employer to collect additional documentation from the employee so that HSI can make a final determination.²⁷ In this case, the employee has ten business days to provide valid work authorization.²⁸ If the employee does not comply, the employer must terminate the employee to avoid fines or potential criminal penalties.

Administrative inspections result in one of the following dispositions:

- **Compliance:** No technical or substantive violations in paperwork and no unauthorized workers are identified, or technical paperwork violations are corrected in a timely manner (adjusted compliance).
- **Warning:** Violations are identified, but there is the expectation of future compliance by the employer.
- **Fine:** The employer has not acted in good faith and has substantive paperwork violations that warrant a fine. (Usually, more than 50% of I-9 forms include substantive errors.)²⁹

If the administrative inspection results in a warning or

fine, a Warning Notice (no fine) or a Notice of Intent to Fine (NIF) will be issued by HSI, as appropriate. The NIF assigns a civil monetary fine to each substantive violation, uncorrected technical violation, and knowing unlawful hire substantive violation.³⁰ The agency will take into account the following factors when assessing the civil fine:

- The size of the business;
- Employer's good-faith efforts to comply;
- The seriousness of the violation;
- Whether the violation involved unauthorized workers; and
- The company's history of previous I-9 violations.³¹

Once issued, attorneys can try to negotiate a reduced fine with an attorney from the ICE Office of Chief Counsel.³² Depending on the circumstances of each case, other consequences for employers include criminal prosecution and debarment of federal contracts or benefits. Employers may also request an appeal hearing with regard to the agency's findings with an administrative law judge (ALJ) at the U.S. Department of Justice.³³ Many such cases, however, never reach the evidentiary hearing stage because the parties either reach a settlement or the ALJ reaches a decision on the merits through dispositive prehearing rulings.³⁴

Impact of E-Verify

The Illegal Immigration Reform and Immigrant Responsibility Act (IIRAIRA) of 1996 authorized the DHS to create an online system that allowed registered employers to quickly verify employment eligibility.³⁵ Since 1 December 2004, E-Verify, a voluntary web-based tool developed for such a purpose and managed by the USCIS, has been an option for employers nationwide.³⁶ According to the USCIS website, as of 15 July 2015, more than 600,000 employers are participating in the E-Verify program.³⁷ In order to participate in E-Verify, an employer must sign a memorandum of understanding

Worksite Enforcement, continued

(MOU), which is a contract between the employer and the DHS.³⁸ The contract is quite detailed and non-negotiable, and lists the responsibilities of the contracting parties. By signing, the employer agrees to “cooperate with DHS and SSA in their compliance monitoring and evaluation of E-Verify, which includes permitting DHS, SSA, their contractors and other agents, upon reasonable notice, to review Forms I-9 and other employment records and to interview [the company] and its employees regarding the Employer’s use of E-Verify, and to respond in a prompt and accurate manner to DHS requests for information relating to their participation in E-Verify.”³⁹ The employer also agrees to use E-Verify for all new employees.⁴⁰ Before signing the MOU, attorneys should advise employers that “DHS reserves the right to conduct Form I-9 compliance inspections, as well as any other enforcement or compliance activity authorized by law, including site visits, to ensure proper use of E-Verify.”⁴¹

E-Verify cannot be used by employers to screen prospective employees, to verify employees with temporary work authorization who require I-9 verification, or to check existing employees.⁴² Employers enrolled in E-Verify enter the employee’s name, date of birth, social security number (required for E-Verify), citizenship status, hire date, document title, document type, document number, and expiration date, where applicable. Employers must submit the employee’s information online to E-Verify within three days of the employee’s hire date.⁴³ Once the new hire’s information is submitted, most employers will receive employee work authorization verification within seconds, as the information is compared against records contained in DHS or SSA databases. If neither the DHS nor the SSA can confirm work authorization within twenty-four hours, the employer receives a tentative non-confirmation.⁴⁴ The employee then has eight federal government working days to contest or resolve the non-confirmation finding.⁴⁵ If he or she does not do so, at the end of the period, E-Verify issues a final non-confirmation notice and the employer must terminate the employee under the terms of the MOU.⁴⁶

In the Form I-9 context, it is important to note that

E-Verify is not a substitute for the Form I-9 but is a supplementary verification process. Thus, employers are not released from the requirements and liability attached to Form I-9. In fact, the MOU specifically states that although the employer participates in E-Verify, “the Employer has a responsibility to complete, retain, and make available for inspection Forms I-9 that relate to its employees, or from other requirements of applicable regulations or laws, including the obligation to comply with the antidiscrimination requirements of section 274B of the INA with respect to Form I-9 procedures.”⁴⁷ There are also some important differences between Form I-9 and E-Verify requirements. Form I-9 is mandatory while currently E-Verify is voluntary for most businesses (unless the employer is the beneficiary of a government contract); Form I-9 does not require a social security number while E-Verify does; Form I-9 does not require photo identification documents while E-Verify does; and Form I-9 must be used to re-verify expired employment authorization while E-Verify specifically states the program cannot be used for that purpose.⁴⁸

One of the benefits of participating in the E-Verify program, besides the almost immediate confirmation of a new employee’s eligibility to work, is that “When an Employer confirms the identity and employment eligibility of newly hired employee using E-Verify procedures, the Employer establishes a rebuttable presumption that it has not violated section 274A(a)(1)(A) of the Immigration and Nationality Act (INA) with respect to the hiring of that employee.”⁴⁹

Participation in the program does not immunize the employer from audits or raids. In fact, the employees’ biographic information entered into the database is immediately available and can be shared with ICE or other government agencies for future enforcement action.⁵⁰ A participating business’s employment records are in plain view of ICE and other government agencies, so enrollment in E-Verify may amplify any Form I-9 errors/violations, such as timeliness issues, procedural errors, or the acceptance of invalid documents. As a result, E-Verify employers may be subject to a higher rate of ICE audits and Notices of Inspection than normal,

Worksite Enforcement, continued

as the USCIS uses algorithms to detect patterns of potential program misuse and takes appropriate action when instances of potential misuse are detected.⁵¹ For example, the USCIS monitors and commences compliance actions in response to the following behaviors: multiple uses of a social security number; employer's failure to use E-Verify on all new hires; failure to contest tentative non-confirmations (TNCs); employer's failure to verify within three days of hire; and employer's impermissible verification of existing employees.⁵²

Employers should procure the assistance of attorneys to help guide them with the internal audit process of their I-9's before enrolling in E-Verify, as doing so may put the company at a higher risk of audits and worksite enforcement if violations are present. I-9 enforcement is bound to become a more prevalent topic under the current administration, and attorneys should be aware of these issues in order to properly advise their clients.



Larry S. Rifkin is the managing partner of Rifkin & Fox-Isicoff PA. The firm's specialty is immigration law and has its principal office in Miami, Florida. He is also the co-chairperson of the USCIS, ICE, CBP, EOIR, Labor, and State Department Liaison Committee Report.

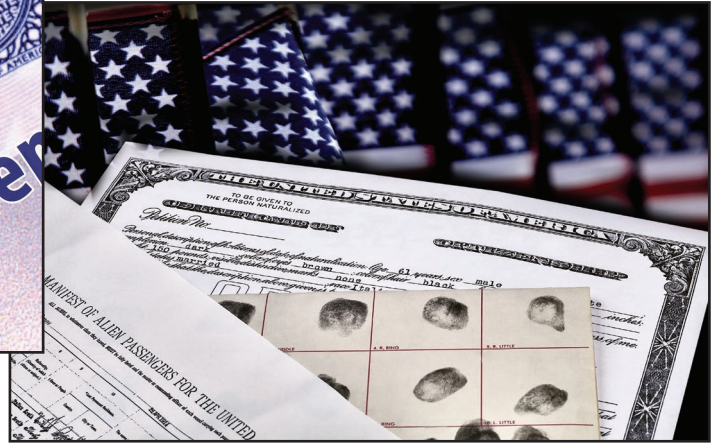
Endnotes

- 1 <https://whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>.
- 2 <https://www.theblaze.com/news/2017/02/10/over-60-percent-of-illegal-immigrants-in-us-live-in-20-cities-most-of-them-sanctuary-cities/>.
- 3 <https://www.numbersusa.com/blog/trump-budget-lays-groundwork-national-e-verify>.
- 4 <https://www.ice.gov/worksite>.
- 5 *Id.*
- 6 Officer of Inspector General (OIG), Department of Homeland Security Memorandum: "U.S. Immigration and Customs Enforcement's Worksite Enforcement Administrative Inspection Process" at page 1 (11 February 2014).
- 7 Pub. L. 99-603, 100 Stat. 3445 (Nov. 6, 1986).
- 8 *Id.*
- 9 *Id.*
- 10 <https://www.uscis.gov/i-9>.
- 11 <https://www.uscis.gov/i-9-central/whats-new>.
- 12 <https://www.uscis.gov/i-9>.
- 13 *Id.* at page 5.

- 14 *Id.* at page 4.
- 15 *Id.* at pages 5-7.
- 16 *Id.* at page 12.
- 17 *Id.* at pages 12-13.
- 18 *Id.* at page 14.
- 19 OIG Memo at page 4.
- 20 <https://www.ice.gov/factsheets/i9-inspection>.
- 21 *Id.*
- 22 *Id.*
- 23 *Id.*
- 24 *Id.*
- 25 *Id.*
- 26 *Id.*
- 27 *Id.*
- 28 *Id.*
- 29 OIG Memo at page 5.
- 30 <https://www.ice.gov/factsheets/i9-inspection>.
- 31 <https://www.ice.gov/factsheets/i9-inspection>.
- 32 OIG Memo at page 9.
- 33 <https://www.ice.gov/factsheets/i9-inspection>.
- 34 *Id.*
- 35 Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), Pub. L. 104-208, 110 Stat 3009 (30 September 1996).
- 36 <https://www.uscis.gov/e-verify/about-program/history-and-milestones>.
- 37 *Id.*
- 38 <https://www.uscis.gov/e-verify/publications/memos/publications-memorandums>.
- 39 https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/MOU_for_E-Verify_Employer.pdf, pages 4-5.
- 40 *Id.* at page 2.
- 41 *Id.* at page 3.
- 42 E-Verify Memorandum of Understanding, www.uscis.gov/files/native_documents/MOU.pdf at 4.
- 43 Government Accountability Office (GAO), "Immigration Enforcement: Preliminary Observations on Employment Verification and Worksite Enforcement Efforts" at 4 (21 June 2005).
- 44 <https://www.uscis.gov/e-verify/what-e-verify/how-e-verify-works>.
- 45 <https://www.uscis.gov/e-verify/employers/tentative-nonconfirmations/dhs-tncs>.
- 46 *Id.*
- 47 https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/MOU_for_E-Verify_Employer.pdf, page 2.
- 48 <https://www.uscis.gov/e-verify/what-e-verify/e-verify-and-form-i-9>.
- 49 https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/MOU_for_E-Verify_Employer.pdf, page 2.
- 50 <https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify/USCIS-ICE-E-Verify-MOA.pdf>.
- 51 <https://www.dhs.gov/news/2011/02/09/testimony-us-citizenship-and-immigration-services-associate-director-theresa-c>.
- 52 *Id.*

The Bitter Side of *Ius Pecuniae* in the United States: Risks Facing EB-5 Investors

By Jeffrey C. Schneider and Marcelo Diaz-Cortes, Miami



Enacted by Congress in 1990,¹ the United States Citizenship and Immigration Services' EB-5 Immigrant Investor Program marks the United States' participation in a popular trend for countries seeking economic stimulus: open arms toward foreigners with deep pockets. Dubbed *ius pecuniae* by international academics,² some countries offer an independent and usually more effective residency process for foreigners willing to risk a substantial investment in the host country. The country's goal is economic progress; the foreign investor's goal is legal residency in the host country and, to varying degrees, a return on investment. The United Kingdom, for example, has a tiered system where the amount of money invested in the county dictates the number of years the investor must wait before requesting permanent residency.³

The United States' iteration of *ius pecuniae*, the EB-5 program—which, in turn, is named after the employment-based fifth preference visa received by its participants—can be described and understood in simple terms. Under the EB-5 program, hopeful immigrant investors, along with their spouses and unmarried children, can obtain permanent residency in the United States if they invest the requisite amount of funds in a commercial enterprise in the United States and, through that enterprise, create or maintain at least ten full-time jobs in the United States for a minimum of two years.⁴ With the immigration nuances handled by immigration

attorneys and others advertised as EB-5 specialists, management of the commercial aspects of the process is often left to domestic businesses charged with ensuring the investor's funds are used in accordance with the program requirements (i.e., to create sustained full-time jobs). Unfortunately, this system sometimes creates the perfect recipe for imperfect information and barriers to intervention by investors. And with large sums of money at stake, the possibility of falling into a mire of misuse or fraud stalks the foreign investors seeking a new home.

Nature and Structure of EB-5 Investments

To qualify for permanent residency under the EB-5 program, hopeful participants must usually invest at least \$1 million in capital in such a way that creates at least ten full-time jobs for United States workers. If, however, the investment is for principal use in a qualified "targeted employment area" (i.e., a rural area with a high unemployment rate), an investor need only invest \$500,000. There is no rigid rule dictating how EB-5 participants must structure their investments or how the investor businesses must operate. The United States Citizenship and Immigration Services (the U.S. CIS) simply requires that the investment be in a "commercial enterprise," with the bulk of the business-related rules focusing on the program's job creation

Risks Facing EB-5 Investors, continued

goals.⁵ A commercial enterprise can take the form of a corporation, business trust, sole proprietorship, partnership, or other business entity (which may be privately or publicly owned). The commercial enterprise must be formed to generate profit, and must set forth a business plan and provide evidence concerning the required job creation.

For investors less inclined to take an active role in the planning and management of the enterprise—which is often most attractive for foreign investors—the U.S. CIS and related regulations allow for pooled investments. That is, one commercial enterprise can be used by various program participants, along with nonimmigrant investors, provided that each program participant invests the required funds and such funds create the required jobs. While the U.S. CIS indeed requires that a program participant actually engages in the management of the commercial enterprise, this requirement appears more relaxed in practice. Under applicable regulations,⁶ the program participant can either be involved in day-to-day direct management or general policy-making activities. The latter leaves great ambiguity and effectively takes the teeth out of the provision. This same regulation also provides that if the enterprise is structured as a limited partnership, all that is necessary is for the investor to have the same rights, powers, and duties provided by the Uniform Limited Partnership Act; whether the investor exercises or even knows about these rights is a separate issue. Accordingly, foreign investors seeking the residency benefits of the EB-5 program, but not the time commitment and stress associated with running a business, often opt for participation in a pooled investment that is managed by a domestic business partner. In theory, such a structure is a “win-win” for all parties: the United States realizes job creation; the foreign investor receives permanent residency and benefits from his or her investment with minimal effort; and the domestic business manager shares in the fruits of a valuable enterprise. Yet, practical barriers inherent in this system leave foreign investors vulnerable to inept business partners and outright scammers.

Practical Limitations Plaguing Foreign Investors

The pooled, hands-off commercial enterprise is most

attractive for foreign investors and has gained popularity in the United States. Unfortunately, this structure brings with it the potential for misuse, misappropriation, and waste of investor funds. Most EB-5 plan participants do not have the social or professional network enjoyed by domestic investors. Foreign investors likely have few contacts in the United States and do not feel confident questioning or analyzing the domestic business partner managing the enterprise. Rarely will foreign investors be on a level playing field with enterprise managers when it comes to legal and financial know-how in the United States. Nor will most foreign investors have the unbridled ability to oversee or, more importantly, fully understand the intricacies of the operations of the enterprise in which they have invested. While foreign investors usually engage professionals in the EB-5 arena, these professionals often have working relationships with domestic business managers or work for finder’s fees, resulting in different motivations with respect to the projects.

In addition, an investor’s limited understanding of the business structure in which he or she has invested and misconceptions as to the legal, economic, or immigration consequences of asserting investor rights may stall or deter an investor from taking an active role in managing or protecting his or her investment. When faced with red flags, a foreign investor may sit idle for fear of destabilizing the project or jeopardizing chances at permanent residency. Other investors, having heard about the litigious nature of the United States, may fear being sued in the United States for intervening or speaking out against the business manager. Others may fear general retribution—legal or otherwise—from the business manager. Some foreign investors are plainly naïve, thinking that their investment is safe simply because it is in the United States and is related to what they perceive to be official government business (i.e., immigration). Lastly, language and cultural barriers create an implicit obstacle to a full understanding of the nature of the business by foreign investors.

Understanding the foreign investors’ practical shortcomings from the outset, or having learned it after some experience, domestic business partners can exploit the disconnect in a number of ways. They can engage in self-serving transactions with related entities, use funds

Risks Facing EB-5 Investors, continued

for personal items or services, overcharge management fees, or simply siphon off funds. The lingual, professional, and geographical divides allow domestic managers to hide or disguise troubling aspects of the commercial enterprise. Thus, whether a domestic manager intended to defraud or misuse investor assets from the outset, such a scheme becomes a tempting option once the manager realizes the amount of money being handled and the ease with which it could be mishandled.

Job Creation, Compliance, and Fiscal Responsibility Can Prove Difficult to Reconcile

At the same time, EB-5 projects present incompatible goals and incentives. The U.S. CIS's job creation requirement compels the hiring of U.S. workers to work for the enterprise, whether or not the labor is actually needed. The business manager must keep the foreign investors content by focusing on job creation for the few years required by the U.S. CIS for permanent residency, but does not focus on long-term sustainability for the enterprise. As a consequence, business managers can deploy funds for goods, services, or even projects that do not make economic sense but create the requisite number of jobs. As an example, a business manager may use investor funds to build facilities that will never yield a return great enough to justify the expenditure. Similarly, compliance with applicable tax and securities regulations may be of lesser priority to the business managers, who must trace direct job creation to specific investor funds while managing the pooled funds. The business manager might value generating evidence of job creation over generating clean accounting entries or a business model that seeks profits over mere job creation.

When the Chickens Come Home to Roost: The EB-5 Imbroglia

The foregoing is not a theory. These elements have indeed combined to create some nightmares for foreign investors. And when the music stops playing, the EB-5 participants are faced with legal, regulatory, financial, and emotional difficulties of the type not previously experienced by the foreign investors. Sometimes the projects simply run out of money; other times regulators intervene and seize control of the enterprise. In either

instance, the foreign investors must deal with issues on all fronts. They must attempt to recoup what they can of their investment; salvage their hopes of permanent residency; and address the legal and regulatory liabilities of the enterprises of which they are legally a "business partner." Meanwhile, the government intervenes with civil enforcement actions and, sometimes, criminal proceedings against the domestic business managers. The result is a complicated legal and regulatory melee that could include court-appointed fiduciaries, investor class actions, angry trade creditors, suits against third parties, and perhaps most troublingly, uncertainty regarding residency. Examples of this unfortunate result can be found throughout the country: the Jay Peak proceedings (Florida/Vermont);⁷ the San Francisco Regional Center proceedings (California);⁸ the Chicago Convention Center proceedings (Illinois);⁹ and the Aero Space Port International Group proceedings (Washington).¹⁰

With each case presenting different facts and problems facing the aggrieved investors, there is no guidebook for courts to determine proper relief. Even where a responsible party, such as a receiver or a regulatory agency, steps in to unscramble the mess left behind, the aforementioned competing interests (e.g., job creation versus preservation of the estate) further complicate matters relating to disposition of remaining property and settlement with other parties. The result is a series of legal proceedings that could take years to resolve.

Advice for Prospective EB-5 Participants

There is no known deterrent for fraudulent or inept business partners. The best advice for an investor is to treat an EB-5 investment like any other business venture. Due diligence is key, and ongoing, active management and oversight by the investor can go a long way in identifying and acting upon red flags and even deterring impropriety. In this regard, investors should seek trusted, independent professionals to help evaluate a potential EB-5 investment and maintain review of the enterprise's operations. EB-5 "specialists" and project managers comprise a relatively small community, with loyalties, possible commissions, and self-interest potentially affecting the partiality of opinions given to foreign investors.

Risks Facing EB-5 Investors, continued

Second, if something appears wrong, the investor should not hesitate to consult an attorney and exercise appropriate investor rights. The United States legal system provides useful protections, and fear of interference with the enterprise or retribution from others should not discourage action when important questions remain unanswered by those managing the enterprise.

Finally, to the extent possible, investors should seek added investor protections baked into the enterprise structure. This may take the form of ongoing and liberal financial disclosure obligations on the part of the business manager, an executive or a managerial position elected by the investors to represent their interests, or even ongoing oversight by a neutral third party, such as a law firm or an accounting firm.

Conclusion

ius pecuniae is a useful and direct immigration policy for countries and investors that know what they want. Nonetheless, countries, including the United States, must ensure that their immigration program does not facilitate failed or fraudulent business endeavors. United States lawmakers are taking aim at the EB-5 program as it currently exists. Some seek to eliminate the program in its entirety¹¹ while others seek to increase the investment requirement while adding fraud prevention and recovery mechanisms.¹² Given the current political climate and the acknowledged need to curb the opportunity for misuse and fraud, hopeful immigrants can expect changes to the EB-5 program. Whatever those changes may ultimately be, however, should not affect foreign investors' resolve to stay informed and involved in their business endeavor and to take action when necessary to protect their interests.



Jeffrey C. Schneider is a founding partner and current managing partner of Levine Kellogg Lehman Schneider + Grossman LLP in Miami, Florida. He is a trial lawyer whose practice focuses on complex commercial litigation, receiverships, and international arbitration. He has worked on some of the

largest fraud cases in history, either as lead trial counsel, as receiver, or as special counsel to the receiver. He

has helped to recover over \$100 million for defrauded victims, and is considered an expert on Ponzi schemes.



Marcelo Diaz-Cortes is an associate attorney at Levine Kellogg Lehman Schneider + Grossman LLP in Miami, Florida. He focuses his practice on complex commercial litigation, bankruptcy, and receiverships. He has assisted clients in a variety matters ranging from

commencement of international insolvency proceedings under Chapter 15 of the United States Bankruptcy Code to serving as local collections counsel for a judgment against a foreign billionaire family. He has also advocated on behalf of and against court-appointed receivers in both state and federal proceedings.

Endnotes

- 1 Immigration Act of 1990, Pub L. No. 101-649, 104 Stat. 4978 (1990).
- 2 Jelena Dzankic, *Citizenship with a Price Tag: The Law and Ethics of Investor Citizenship Programmes*, 64(4) N. IR. LEGAL Q. 387, 388 (2014).
- 3 UK VISAS & IMMIGRATION, TIER 1 (INVESTOR) OF THE POINTS BASED SYSTEM – POLICY GUIDANCE 38 (12/2016 ed.), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/577675/T1__I__Guidance_12_2016.pdf.
- 4 8 C.F.R. § 204.6(j)(4) (2017).
- 5 See generally 6 U.S. CITIZENSHIP & IMMIGRATION SERVICES, POLICY MANUAL, pt. 6, Ch. 2 (2017) available at <https://www.uscis.gov/policymanual/HTML/PolicyManual-Volume6-PartG-Chapter2.html#S-A>.
- 6 8 C.F.R. § 204.6(j)(5).
- 7 *SEC v. Quiros et al.*, Case No. 1:16-cv-21301 (S.D. Fla.) and related cases.
- 8 *SEC v. San Francisco Regional Center LLC et al.*, Case No. 3:17-cv-00223 (N.D. Cal.).
- 9 *U.S. v. Sethi*, Case No. 1:14-cr-00485 (N.D. Ill.) and related cases.
- 10 *SEC v. Chen et al.*, Case No. 2:17-cv-00405 (W.D. Wash.).
- 11 Press Release, Senator Chuck Grassley, Feinstein, Grassley Introduce Legislation to Eliminate Troubled EB-5 Investor Visa Program (3 Feb. 2017), available at <https://www.grassley.senate.gov/news/news-releases/feinstein-grassley-introduce-legislation-eliminate-troubled-eb-5-investor-visa>.
- 12 See e.g., Kevin Penton, *House Judiciary Committee Calls for EB-5 Reforms*, LAW360 (8 Mar. 2017), <https://www.law360.com/immigration/articles/899203>; Allissa Wickham, *Examining Goodlatte's EB-5 Bill, As Deadline Looms*, LAW360 (16 Sept. 2016), <https://www.law360.com/articles/840663/examining-goodlatte-s-eb-5-bill-as-deadline-looms>; Kelly Knaub, *GOP Rep. Goodlatte Pushes for EB-5 Reform Bill*, LAW360 (12 Sept. 2016), <https://www.law360.com/articles/838754/gop-rep-goodlatte-pushes-for-eb-5-reform-bill>.

The Impact of International and U.S. Domestic Law on the Future of the Global Medical Marijuana Market

By Benjamin R. Rosenberg, Miami

During the 2016 election cycle in the United States, voters from five states voted to legalize marijuana for medical use. This brings the total number of states where medical marijuana is legal to twenty-eight. Right now, lawmakers from these states are in the process of deciding how these new laws will be implemented on the state and local levels. Despite the fact that medical marijuana is legal, the states, let alone the local municipalities, still have not agreed on an

approach to regulate the industry, which only creates more confusion in the market for both corporations and consumers. This process has created a lack of national homogeneity in the United States for the approach to deal with the movement toward legalization.

The United States is quickly moving toward legalization in all fifty states and, with a lack of direction on the federal level, three major hurdles may impede the forthcoming international growth of the industry. First, there are several international treaties in place that limit and/or prevent the international trade of cannabis and its related products. Second, current Drug Enforcement Administration (DEA) scheduling creates a litany of problems, but the alternative to rescheduling may actually lead to a worse outcome. Lastly, traditional banking and investing in cannabis-related businesses create several unique problems given the international and domestic limitations created by treaties and the DEA.



International Treaties That Govern Drug Control

It is impossible to have a discussion regarding the international implications of medical marijuana without first looking into the existing treaties that govern the way countries approach this issue. In order to do so, it is important to delve into the basics of the international drug control treaties and how they may apply to the issue at hand.

Present-day international drug control is influenced mainly by the 1961 Single Convention on Narcotic Drugs (Single Convention), which was preceded in 1912 by the International Opium Convention. The old system was replaced in 1961 by the Single Convention when it became clear to the member countries that there was a need to start with a clean slate to deal with shifting international challenges—a period we may be entering into now. The Single Convention, along with the 1971 Convention on Psychotropic Substances (CPS) and the

Future of the Global Medical Marijuana Market, continued

1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UN Convention), forms the basis of the global drug control regime as it exists today.

The main thrust of the Single Convention is to control, and protect against, the use and possession of opiates, cannabis, and cocaine.¹ Specifically, it prohibits possession or cultivation of the above drugs in any form in addition to creating a classification system (dividing the predefined drugs into four schedules) and establishing the International Narcotics Control Board (INCB).² The classification system acts to establish differing degrees of regulation for each schedule and serves as the model for most national scheduling systems.³ The INCB acts as the governing body for the Single Convention and is tasked with monitoring treaty compliance among the signatory nations.⁴

In addition to the Single Convention, the CPS has a direct bearing on international control of narcotics and psychotropic substances.⁵ The CPS was enacted as a result of an uptick in drug use in the 1960's and added certain drugs—like LSD—to the list of controlled substances.

Lastly, the UN Convention was created as a response to the increase in drug trafficking. The UN Convention was the first drug enforcement treaty to require its member countries to create and enforce laws that punish individuals for drug possession and personal consumption. Interestingly, the UN Convention did not specify how punishments were to be doled out, only that member countries “shall take appropriate measures to prevent illicit cultivation of and to eradicate plants containing narcotic or psychotropic substances, such as opium poppy, coca bush and cannabis plants, cultivated illicitly in its territory.”⁶

The above three international treaties are not self-executing, although they constitute the basis for international law concerning the control of drugs. Further, these treaties are considered legally binding,⁷ but as with every treaty, enforceability remains a concern.

Given that there has been no formation of an international police department, the INCB and member countries are only able to enforce the treaties by applying political pressure to any detractors. This could take the form of shining a light on the member countries' lack of compliance with the treaty through the media. In some extreme cases, pressure may be applied through embargos on imports and exports coming into or going out of a country, or reducing foreign aid.

International Governing Bodies

In the minds of most, the United Nations (U.N.) often exists outside of the purview of most people. Therefore, it should come as no surprise that the general perception is that the U.N. and international law do not really do much that would influence nation states' internal decisions relating to their laws and policies. Nothing could be further from the truth, especially as it relates to the impact that international laws have on the cannabis business.

Currently, the international drug control treaties are governed by three U.N. organizational bodies. The Commission on Narcotic Drugs (CND), which consists of delegates from fifty-three countries, is the main governing body. In its annual meetings, the delegates review policies that were enacted pursuant to the treaties and provide guidance for proper implementation of current and future policy. The United Nations Office on Drugs and Crime's (UNODC) prime directive is to implement policies enacted by the CND. The UNODC has an independent budget to create or support drug control programs implemented all around the world. The INCB is tasked with enforcing the treaties. In its role, the INCB publishes an annual report, which for 2016 discussed the issue of women on drugs and the functioning of the international drug control systems.⁸ Further, the INCB reviews major developments in global drug control systems and legislation broken down by regions.⁹ These regulatory bodies act in concert but rely heavily on specific systems that exist in order to ensure the intended implementation and outcome of the dual objective of the treaties, which, in this case, is

Future of the Global Medical Marijuana Market, continued

to eliminate the illegal flow of substances used for illicit purposes, without restricting the flow and availability of necessary medicines.

The Impact of International Laws Domestically

International drug laws have an immense influence on the internal laws and politics of member countries. In fact, international drug treaties are overwhelmingly concerned with the domestic affairs of the member countries and the methods for implementing and furthering the goals they set forth. Member countries are very limited in what they can legally do to enforce the international treaty obligations, despite the rigidity of the policy changes they decide to implement for their own, respective citizens.

In 1970, the United States enacted the Controlled Substances Act of 1970 (CSA). In part, the CSA was created in order to meet the United States' obligations with respect to the scheduling system set out in the Single Convention. In order to maintain congruency, the CSA utilizes an internal mechanism that ensures the scheduling systems in the Single Convention and the CSA continue to directly correspond with one another.

Chuck Rosenberg, acting administrator of the Drug Enforcement Administration, vis-a-vis the powers of the attorney general (now Jeff Sessions), is in charge of scheduling under the CSA. In his position, Mr. Rosenberg is not free to unilaterally reschedule a substance such as marijuana to a less restrictive schedule absent a specific procedure, which is set out below.

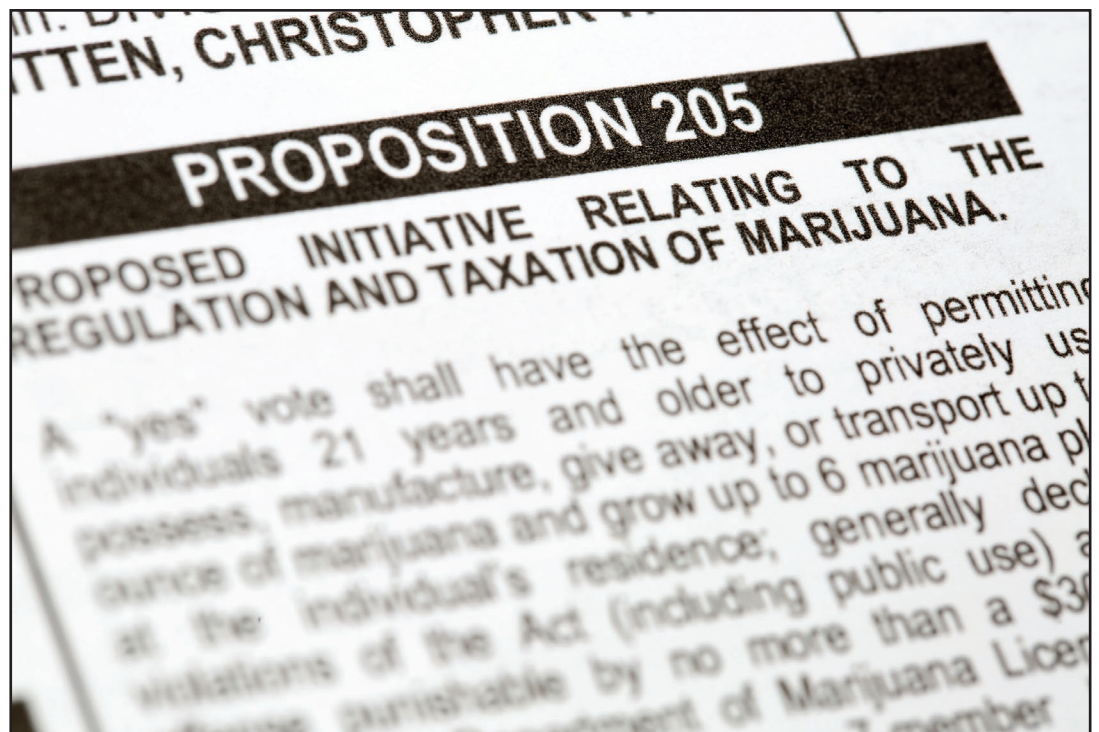
While treaties and international laws are

generally concerned with the implementation of federal law, this fact does not create an exemption for state and local governments from the requirements of the treaty or international law pursuant to the doctrine of preemption.¹⁰ What this means is that although each state has the ability to enact its own drug laws, federal law preempts, or overrides, state law when it covers the same subject matter. In other words, the federal law sets the floor while state and local laws set the ceiling.

Given its very conservative stance on medical marijuana, it seems likely that the Trump administration will lean on the fact that the government is obliged to follow the letter of the treaties in order to fulfill its international obligations, as a way to sidestep the issue. Given that medical marijuana is not a major issue for President Trump and that Attorney General Sessions has taken a hardline conservative stance on the subject, it is unlikely we will see any easing of restrictions at the federal level.

Does the U.S. rescheduling cannabis offer a solution to the international issue?

Despite over half the states in the United States legalizing medical marijuana and numerous petitions,



Future of the Global Medical Marijuana Market, continued

the DEA continues to maintain that cannabis should still be classified as a Schedule 1 narcotic—which consequently deems that cannabis has no accepted medical use. As such, cannabis continues to be subject to the restrictions imposed by the Single Convention and subsequent treaties. It would logically follow that the best solution would simply be to reschedule cannabis.

A substance is rescheduled in one of two ways: (1) congressionally; or (2) through the executive branch.¹¹ Neither is expeditious.

Congress has the power to reschedule cannabis, either by introducing and passing new legislation specific to cannabis or through an amendment to the Controlled Substances Act.

The path to rescheduling, or removing, a substance through the executive branch begins with presenting a petition to the DEA, which is subsequently reviewed internally. If the DEA accepts the petition, it then refers it to the Department of Health and Human Services (HHS) to conduct a scientific and medical evaluation. The HHS follows an eight-factor analysis and compiles an opinion that suggests a course of action. The analysis sets out to determine the following: (1) potential for abuse; (2) scientific evidence of the drug's pharmacologic effect; (3) current scientific knowledge of the drug; (4) history and current pattern of abuse; (5) the drug's scope, duration, and significance of abuse; (6) the risk, if any, to public health; (7) any psychic or physiological dependence liability; and (8) whether the drug is an immediate precursor of a controlled substance.¹² The end result is that the DEA and the attorney general are bound by the decision and recommendation of the secretary of the HHS.¹³

Hypothetically, should cannabis be rescheduled as a Schedule 2 drug, it would then enter the purview of the Food and Drug Administration (FDA). Should this happen, the FDA would likely keep a close eye during manufacturing and could require extensive clinical testing to demonstrate the effectiveness of cannabis. This would effectively scare away investors and, more importantly, further hamstring foreign trade.

International Issues Relating to the Lack of Banking Services

Availability of traditional lending sources and banking services are two of the most important elements to any successful industry, especially when that industry relies on international commerce. Given the current regulatory arena surrounding the cannabis industry, participants are unable to get access to these lending sources or to utilize banking services. As previously stated, cannabis is a controlled substance according to the DEA, which means that monies earned from the sale of cannabis are technically illegal on the federal level. The effect of this is that banks are required under federal law to disclose any and all cannabis-related transactions as suspicious activity. The result of which is that banks that decide to accept these funds are opening themselves up to additional unwanted federal scrutiny and potential seizure of funds by the Federal Deposit Insurance Corporation (FDIC). It should come as no surprise as to why the large multinational banks and investors want no part in the industry. The effect of this is that banks are unable to take deposits from businesses that are involved in the cannabis industry, forcing these businesses to deal solely in cash.

Running a multimillion-dollar cash business creates a litany of problems, not the least of which is security. More important, from an international trade perspective, is the ability to make large-scale purchases and allow for corporate expansion. The hurdles of dealing solely in cash create problems exponentially more difficult to deal with when looking to engage abroad as opposed to domestically. If a U.S. medical marijuana business wants to buy \$100,000 in manufactured goods for its business from a Puerto Rican manufacturer, several questions come to mind that highlight the complexity of this situation. For instance, how is the money supposed to get there? Moreover, is sending money derived from the sale of medical marijuana abroad considered laundering money?

Conclusion

In order to incentivize and propagate the ever-expanding

Future of the Global Medical Marijuana Market, continued

medical marijuana industry, some of the influential member states to the treaties need to be more vocal. They need to make a point about how they see this burgeoning industry growing and what vehicles, if any, will be put in place to allow for trade to occur more freely. As it stands, Latin America and the United States—and really any other member country for that matter—are unable to participate in trade for medical marijuana goods. Further, with the current restrictions in banking, large-scale recurring transactions are unsustainable. As a result, by easing some internal restriction, the United States may be able to start the larger picture discussion with its most obvious trade partner in this industry, Latin America.



Benjamin R. Rosenberg is the founding partner of Rosenberg PA and has experience representing clients in the areas of complex business litigation, with a focus on domestic and international matters, and corporate transactional law. He

also provides business consulting in the area of medical marijuana for both businesses and investors.

Endnotes

- 1 Single Convention on Narcotic Drugs, 30 March 1961, 14 I.L.M. 302.
- 2 *Id.*
- 3 *Id.*
- 4 *Id.*
- 5 Convention on Psychotropic Substances, 21 February 1971, 10 I.L.M. 261.
- 6 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988, 28 I.L.M. 493.
- 7 This is pursuant to the 1969 Vienna Convention on the Law of Treaties, which generally states that a country may not circumscribe its obligations under the treaties by enacting a conflicting domestic law. See 8 I.L.M. 679.
- 8 International Narcotics Control Board, Annual Report (2016), https://www.incb.org/documents/Publications/AnnualReports/AR2016/English/AR2016_E_ebook.pdf.
- 9 *Id.*
- 10 Article VI, Section 2, of the U.S. Constitution provides that the “Constitution, and the Laws of the United States . . . shall be the supreme Law of the Land.” U.S. CONST. art. VI, § 2.
- 11 21 U.S.C. § 811.
- 12 21 U.S.C. § 811(c).
- 13 21 U.S.C. § 811(b).

In addition to being sent to our section database of 1,097 members, the ILQ will be distributed at select events during the year.

CONTACT:

Clarissa A. Rodriguez
crodriguez@tenzer.com or (305) 870-7544

ADVERTISE IN THE ILQ!

WORLD ROUNDUP

ASIA



Robert Q. Lee
robert.q.lee@rimonlaw.com

CHINA

China approves seven new Free Trade Zones.

The State Council released a statement on 31 March 2017 that it had approved seven new Free Trade Zones (FTZs) in the provinces of Liaoning, Zhejiang, Henan, Hubei, Sichuan, Shaanxi, and Chongqing. The statement followed the 31 August 2016 announcement by the Chinese minister of commerce that seven new FTZs would be established in China. The FTZs were launched on 1 April 2017, bringing the total number of FTZs in China to eleven.

Five of the new FTZs are located in the interior of China. Gao Hucheng, the Chinese minister of commerce, stated that this is reflective of the fact that central and western China will be the “new frontier” for foreign investment in China, in line with the country’s One Belt, One Road initiative. Each FTZ will have a specific priority:

- **Liaoning:** to reinvigorate the competitiveness of northeast China’s traditional industries and to establish new sectors for foreign investment;
- **Zhejiang:** to improve the construction of the Zhoushan Free Trade Port and to encourage commodity trade liberalization;
- **Henan:** to establish a modern three-dimensional traffic system and modern logistics system by expediting the construction of north, south, and east infrastructural links; to transform into a state-of-the-art integrated transport hub and become a key location along China’s One Belt, One Road connection with Eurasia;
- **Hubei:** to serve as a hub for high-tech industrial bases focusing on the Yangtze River Economic Belt;
- **Sichuan:** to serve as the gateway to China’s western inland areas and to improve collaboration between interior and coastal areas;
- **Shaanxi:** to facilitate the construction of the One Belt, One Road network; and
- **Chongqing:** to serve as a strategic gateway city in opening up the western region of China and facilitating the region’s overall future development.

Foreign investors will be permitted to establish within the FTZs a wholly foreign owned enterprise (WFOE) rather than being required to partner with a Chinese company in more industry sectors than is permitted outside of the FTZs.

People’s Republic of China establishes new law governing NGOs that operate within mainland China.

China’s new Foreign Non-Governmental Organizations (NGOs) Management Law became effective 1 January 2017, and will affect foreign individuals and organizations in China. Foreign NGOs will be required to register with a government “supervisory unit” and with the Ministry of Public Security. A Handbook for Foreign Non-Governmental Organizations’ Registration of Representative Offices and Filing of Temporary Activities is provided to assist foreign non-governmental organizations in registering representative offices or filing to carry out temporary activities within mainland China.

SOUTH KOREA

South Korea passes anticorruption law.

The Anti-Corruption and Bribery Prohibition Act became effective in September 2016. The Act establishes the maximum amount one can spend on a meal provided to an official at 30,000 KRW. Any of the following requests (made directly or through a third party) will constitute a violation of the Act:

- Request for illegal handling of a public official’s duties relating to permissions, patents, approvals, examinations, certifications, confirmations, etc.;
- Request for reduction or exemption of decertification, fines, penalties, disciplinary action, etc.;
- Actions impacting public official’s personnel decisions, such as hiring, promotions, transfers, etc.;
- Request for unauthorized disclosure of confidential information related to bids, auctions, developments, examinations, taxes, etc.;
- Request for selection of a particular individual, organization, or corporation to (or removal from) the list of parties to a contract against relevant laws;
- Request for the sale, exchange, or transfer of goods or services produced, supplied, or managed by a public institution to a specific individual, organization, or corporation at prices outside of legal limits or market norms; or

- Actions impacting the results or assessments related to decisions or assessments made by public institutions.

The penalty for violation of the Act may result in a fine of up to 30 million KRW and/or up to three years' imprisonment.

SINGAPORE

Singapore enacts laws to improve international dispute resolution.

Singapore passed two laws intended to improve Singapore's international dispute resolution. The civil law amendment bill permits third-party funding in cases involving international commercial arbitration. The mediation bill addresses enforcement of mediated settlements.

Third-party funding is allowed in internationally recognized arbitration centers such as London, Paris, and Geneva. As observed in such arbitration centers, third-party funding will permit commercial funders to enable the funded party to litigate such party's case in Singapore.

The new mediation provision includes several noteworthy provisions. In addition to allowing parties who reach a settlement after mediation to agree to apply to have the settlement recorded as a court order, which can then be enforced, the new mediation law also requires that communications arising out of mediation cannot be disclosed to any third party or admitted into evidence without the parties' permission.

Robert Q. Lee is a partner of Rimon Law with offices in Miami and Orlando, Florida. He represents public, private, and emerging growth companies in corporate and commercial matters, mergers, asset and stock acquisitions and divestitures, reorganizations and roll-ups, business start-ups, securities offerings, indentures, bond issues, corporate governance, private equity and mezzanine financing, securitizations, equipment financing, secured transactions, supplier and distribution agreements, technology licensing, servicing agreements, and franchising.

MIDDLE EAST



Omar K. Ibrahim
omar@okilaw.com

Qatar introduces new arbitration law.

On 16 February 2017, Qatar enacted a new arbitration law (Law No. 2 of 2017). This law replaces Qatar's 1990 arbitration law. While it is in line with the UNCITRAL Model Law on International Commercial Arbitration, it does vary from the Model Law in some respects. Some

of the more notable takeaways are that Qatari public entities may now enter into contracts with arbitration clauses, provided the public entity obtains the requisite authority from the prime minister or his delegate, and that a tribunal's decision on its jurisdiction may be challenged during the arbitral proceedings by an appeal to the relevant Qatari court or the arbitral authority set out in the arbitration agreement. Legal experts and government officials are optimistic that the new arbitration law will benefit the country's construction industry.

Changes to UAE's penal code may damage UAE's status as the Middle East's international arbitration hub.

Late last year (2016), Article 257 of the United Arab Emirates Penal Code was amended to provide that "[a]nyone who issues a decision, expresses an opinion, submits a report, presents a case or proves an incident in favour of or against a person, in contravention of the requirements of the duty of neutrality and integrity, while acting in his capacity as an arbitrator, expert, translator or fact finder appointed by an administrative or judicial authority or selected by the parties, shall be punished by temporary imprisonment [i.e., three to fifteen years]." The amendment has sparked alarms among the arbitration community that arbitrators and experts may be subject to vexatious criminal proceedings by a recalcitrant losing party. While UAE practitioners have counseled it is unlikely that local prosecutors would pursue such actions, absent exceptional circumstances, many international arbitrators seated in the UAE have already resigned from tribunals. Local practitioners and others have requested that the UAE Cabinet of Ministers review Article 257.

Dubai court provides clarification on the res judicata effect of an arbitral award.

The Dubai Court of Cassation recently clarified when an arbitral award has res judicata effect. In a judgment dated 21 August 2016 (Commercial Appeal 199 of 2014), the court held that an award has res judicata effect from the moment it is issued, not when it is confirmed, and the award will only cease to have that effect if, and when, it is annulled. The fact that an award is under review for annulment or confirmation does not mean that it lacks res judicata effect, or that it would only gain res judicata effect once it has been confirmed. In practical terms, the decision clarifies that a party cannot commence a separate action based on a dispute decided by an arbitration award because the award is in the confirmation process.

Jordan's Supreme Court rejects U.S. extradition request.

On 20 March 2017, the Jordanian Supreme Court

affirmed an appeals court decision denying the United States' extradition request for Ahlam Al-Tamimi. Al-Tamimi was convicted in Israel for assisting a suicide bomber to detonate a bomb in Sbarro in 2001 that killed fifteen people, including two Americans. She was released in 2011 by Israel in a prison swap with Hamas and was residing in Jordan. The United States then sought her extradition. The Jordanian courts denied the request on the basis that the Jordanian Parliament never ratified the 1995 Extradition Treaty between the United States and Jordan. Interestingly enough, the U.S. Department of State considers the 1995 Extradition Treaty to be in full force and effect.

Omar K. Ibrahem is a practicing attorney in Miami, Florida.

NORTH AMERICA



Courtney Caprio

ccaprio@sinclairlouis.com

The Russians conduct cyber-invasion of the United States.

The Russians have landed in the United States, albeit via cyberwarfare. Since Donald Trump's ascendency to the presidency—which was a “surprise” result largely missed by the mainstream media—the U.S. intelligence community has been actively investigating links between the Trump campaign and the Russians, as well as the existence of any coordination between the two to influence the 2016 election.

In January 2017, the intelligence community publicly shared its assessment that the Russian government had hacked the Democratic National Committee and Hillary Clinton's presidential campaign chairman to release damaging emails in a bid to sway the election in favor of Trump. During *The Economic Times*' Global Business Summit held on 27 March 2017 in New Delhi, former Vice President Dick Cheney called out the Russians' “cyberattack on the United States,” deeming it “an act of war.” Such an unprecedented cybersecurity infiltration into a presidential election signals a troubling shift that the United States must address via its criminal justice system in addition to the imposition of sanctions, which President Barack Obama ordered on Russia before leaving office.

Encouragingly, the United States is also seeking accountability for malicious international cybercrime through the federal criminal justice system. On 14 March 2017, the U.S. Justice Department announced the indictments of two Russian spies and two Russian

nationals in connection with the hacking of 500 million Yahoo user accounts in 2014. The accused perpetrators allegedly sought the hacked information for intelligence purposes as well as for financial gain. This is the first time the United States has levied criminal cybercharges against Russian government officials. Notably, the indicted FSB officers (Russia's Federal Security Service, a successor to the KGB) worked for the cyberinvestigative arm of the Russian agency. Although unrelated to the Russian hacking of the DNC and its interference with the 2016 presidential election, the indictment nonetheless represents the Justice Department's willingness to use federal criminal law to cast its dragnet over international cybercriminals to hold them accountable within the United States.

Regarding the 2016 election, the Justice Department's investigation into the Trump administration's alleged collusion with the Russian hackers continues, as almost-daily reports continue to surface of dubious pre-election meetings and financial ties between Trump's closest advisors and the Russian government. Whether more federal indictments or additional sanctions against Russia are issued or whether the Republican Congress enacts more targeted legislation to criminalize cyberwarfare remains to be seen. That the United States presidential election can be successfully targeted by cybercrime raises serious issues about data privacy, and represents a new frontier for propaganda that now takes form as fake news on voters' Facebook feeds.

Spokeo and standing: Who can sue in data breach cases?

In *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016), the U.S. Supreme Court ruled that a plaintiff cannot satisfy Article III standing, or satisfy that he has suffered an injury in fact, by alleging a “bare procedural violation” of a statute.

Spokeo is an online “people search engine,” marketed to human resources departments as a screening mechanism that collects information on individuals from different databases. When Thomas Robins, an unemployed resident of Virginia, saw that his profile was blatantly false—stating that he had a graduate degree with a wealth level of the “Top 10%”—he filed a class action, alleging violations of the Fair Credit Reporting Act (FCRA) based on Spokeo's failure to follow reasonable procedures to ensure the accuracy of consumer reports and that the misinformation posted online had harmed his employment prospects.

After the district court dismissed the case for lack of standing, the Ninth Circuit reversed, holding that violation of a private statutory right is sufficient injury in fact to confer standing. The Supreme Court then reversed the Ninth Circuit, holding that standing requires a concrete injury (not just speculative harm to employment prospects), and is not automatically satisfied whenever a statute that grants a private right of action is procedurally violated.

Post-*Spokeo*, a majority of appellate courts have disagreed with the Supreme Court's more restrictive view of injury in fact standing. The Third, Sixth, and Eleventh Circuits have ruled that *Spokeo* does not preclude class actions in which plaintiffs allege their only concrete injury is intangible in data breach cases. Consequently, class action data breach litigation is alive and well, notwithstanding a Supreme Court ruling that could have been a death knell.

When “the cloud” is overseas, even a warrant will not compel turnover of data.

While we are all aware that “the cloud” stores our data, rarely do we consider exactly where “the cloud” is located geographically. It is not in the sky as its name may imply, but rather consists of server farms or data centers owned by Internet service providers (ISPs) housed all over the world.

In *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), the Second Circuit held that even armed with a warrant, the U.S. government cannot compel ISPs to turn over data that is stored on “the cloud,” but is physically located on a server farm overseas. In 2013, a magistrate judge from the Southern District of New York issued a warrant under the Stored Communications Act (SCA) for information associated with a Microsoft Network email address. Microsoft turned over responsive data stored in the United States, but moved to quash the warrant because much of the requested data was stored on its server in Ireland, arguing that it was beyond the jurisdiction of the warrant. The magistrate rejected this argument and was affirmed by the district judge, who held Microsoft in civil contempt for refusing to comply with the SCA warrant.

On appeal, the Second Circuit reversed in favor of Microsoft, focusing on the statute's purpose and application rather than the intangible nature of data itself. The court held that the SCA does not apply extraterritorially, and that compelling Microsoft to produce data stored in Ireland would contravene this limitation. In so holding, the court reasoned that the SCA focused on privacy. The privacy interest was in Ireland; thus, the warrant had no force and effect on the (extraterritorial) Ireland-stored data.

The SCA was enacted in 1986 before Congress could fathom its application to data stored on “the cloud.” Aside from the location of the data being completely fortuitous—note that some content from the email account located on Microsoft's United States server was promptly turned over—the court relied on this one (arbitrary) fact to quash the warrant rather than focus on the intangible nature of data and the location/nationality of the data's creator, which was unknown.

In short, the Second Circuit relied on statutory interpretation in a vacuum by ignoring technology: that

data can physically migrate across servers worldwide, and that the creator has no control over where his data is stored. A better analysis may have been to focus on where the data was created: if the email account holder created the subject emails while within the United States, the warrant could be deemed valid due to jurisdiction over that individual rather than focusing the jurisdictional inquiry on the haphazard (and fleeting) location of the data he created.

Courtney Caprio is counsel at Sinclair, Louis & Zaverchnik PA in Miami, Florida. Her practice focuses on media and entertainment law, as well as business litigation. In addition to litigating, she counsels clients on an array of transactional matters, including the protection of intellectual property, business structuring, and employment issues.

RUSSIA



Yana Manotas Mityaeva
yana@manotaslaw.com

Constitutional Court rules that ECHR's *Yukos* ruling cannot be enforced.

On 19 January 2017, the Constitutional Court of the

Russian Federation announced its controversial decision that Russian authorities are not required to comply with a Strasbourg-based tribunal's decision to pay compensation of €1.8 billion to former Yukos shareholders. According to the Constitutional Court, the Resolution of the European Court of Human Rights (ECHR) in the case of *Yukos v. Russia* cannot be enforced because it infringes the rights of citizens of the Russian Federation, ignores the provisions of the constitution of the Russian Federation, and does not take into account the historical aspects of the dispute.

Two years ago, the ECHR ordered Russia to pay unprecedented compensation to former Yukos shareholders for violating their rights in the bankruptcy proceedings of the oil company. The Ministry of Justice considered that by its decision, the Strasbourg tribunal violated the principle of fairness and legal equality, and the Constitutional Court took the side of the Russian authorities. While voicing the opinions, the chairman of the Constitutional Court Valery Zorkin announced, “The ECHR ruling does not abolish the priority of the Constitution for Russia.” Thus, the state has the right to withdraw from the duties imposed on it, if it is the only way not to violate the constitution.

The reasoning of the Constitutional Court is that the decisions of the ECHR (which, in fact, are interpretations

of the Convention for the Protection of Human Rights and Fundamental Freedoms) cannot conflict with the provisions of the Constitution of the Russian Federation guaranteeing the rights and freedoms of its citizens, as well as the established constitutional meaning of other Russian laws.

Addressing the issue of compensation in the *Yukos* case, the Constitutional Court also considered it necessary to take into account the historical facts associated with the development of the Russian tax system and the fiscal peculiarities of the *Yukos* business. The Constitutional Court proceeded from the basis that the national specificity of human rights is enshrined in the Constitution of the Russian Federation and acts of the Constitutional Court of the Russian Federation. The Constitutional Court stated that the ECHR does not always take into account the Russian “constitutional identity” and the historical aspects of the problem that form the basis of the dispute. This approach, it said, leads to a violation of the balance and infringement of public interests, which are mistakenly perceived as the interests of state bodies and officials, when in fact they are a combination of private interests.

The decision was not unanimous; Justices Vladimir Yaroslavtsev and Konstantin Aranovsky of the Constitutional Court expressed dissenting opinions.

“The request is not admissible, and the proceedings in the case were to be terminated,” said Yaroslavtsev in his commentary. He focused on the contradictory nature of the actions of the Russian authorities. “ECHR even in 2011 recognized the violation of the rights of shareholders of *Yukos* by Russia, and then our country did not challenge this decision. In addition, in 2013 the Russian authorities sent a plan of action to the Committee of Ministers of the Council of Europe to implement this resolution. And only in 2014, when Strasbourg announced a record amount of compensation of €1.86 billion, the tactics of the Russian Federation have changed dramatically.”

This “inconsistent and very contradictory position” of the Russian authorities has essentially led to a “legal dead end” of the issue in this case, the justice added. And the Justice Ministry, he continued, found a “simplified” way out by contacting the Constitutional Court with a request that the ECHR ruling could not be executed. This appeal should not stand, according to Yaroslavtsev, due to the principle of *nemo iudex in propria causa* (no one can be a judge in one’s own case), since the Strasbourg tribunal’s finding of a breach of the Convention was largely due to the violation of the principle of legality by a decision of the Constitutional Court on 14 July 2005.

According to Aranovsky, the request itself makes it seem as if “the Constitutional Court is capable of overturning the acts of European justice or, like an arbitrator, to settle differences between the applicant and the ECHR. But for

such a review or arbitration decision, the constitutional analysis has no application, and the court is not obliged to assess either the European justice or the behavior of the Russian representatives, correct their errors, resolve disputes over facts or qualifications, and put the justices’ understanding of the Convention above the ECHR interpretations.”

Yana Manotas Mityaeva is an attorney focused on real estate and business law. A native Russian speaker and fluent in English, she has experience in assisting multinationals with their real estate and corporate holdings, private asset protection, and estate planning across borders. She is vice president of the Russian-American Bar Association of Florida.

SOUTH AMERICA



Mariana Matos

mariana.matos@hlconsultoria ltda.com.br

Latin America increases collaboration in anticorruption enforcement.

We are seeing a global effort to combat corruption and bribery. In Latin America, governmental agencies have begun to improve anticorruption enforcement. A corruption investigation of a multinational corporation often has the potential to involve several domestic anticorruption laws. In this context, it is important to observe measures to secure data privacy of documents and information obtained during investigations in order to avoid any improper disclosure and violation.

Considering that exchange of information among countries is common, companies and their lawyers must protect a company’s data in the most effective way. When a company is under investigation, it is important to comply with local laws related to data privacy. Laws related to data privacy are relevant since they apply to all categories of processing and not only to processing of employees’ data. Therefore, it is important to understand the laws related to data privacy before beginning an investigation or a review of any data to avoid violations that could result in inadmissibility of evidence, fines, or criminal and civil liabilities.

It is essential for a company to take into account the totality of relevant data protection requirements and to document the decisions behind the procedures followed in an investigation. Some of the measures companies can take to protect their data are limiting the investigation in terms of time, scope, and search terms and conducting the investigation in one country to avoid cross-border data transfers. Additionally, maintaining privilege can be vital to protecting a company’s interests, and considering

that privilege rules differ from country to country, it is important to observe the rules in each of the countries where the company and its subsidiaries are located.

In Latin America, we are seeing an intensive collaboration and coordination between several regulators in cross-border matters related to corruption and bribery. The Brazilian Operation Car Wash has resulted in more than 100 international cooperation requests since 2014.

As an example, at the end of 2016, the multinational construction company Odebrecht entered into agreements with authorities in Brazil, Switzerland, and the United States in order to resolve its corruption cases.

The success of these investigations and the cooperation of enforcement authorities in several countries in large part has been a result of intensive information gathering. In this sense, it is important that a company comply with all local laws in order to make certain all employees adhere to the company's general and global strategies.

Cybersecurity strategies increase in Latin America.

Employment of cybersecurity strategies has been increasing at the international level, especially in Latin America. The globalization of business has brought strategic expansion opportunities as well as a broad selection of regional risks. While these risks are manageable, considering the rapid pace of technological innovation, such risks require the attention of each country's leaders.

Each day it is more difficult to safeguard intellectual

property, and this protection is a critical corporate concern for long-term growth and survival. Cybersecurity strategies have been developed recently with the purposes of reinforcing the security and stability of global resources, protecting society against cyberthreats, and bringing social and economic prosperity.

Countries in Latin America continue to prioritize the development of cybersecurity strategies. In this context, defining cybercrimes and legislating penalties are main concerns, and these countries are updating current laws or creating new ones. Brazil, for instance, has approved the Civil Rights Framework for the Internet (*Marco Civil*), which is related to subjects such as the protection of fundamental rights online, intermediary liability, responsibilities of the public sector, and data retention.

In addition to the efforts of governments to implement cybersecurity strategies, it is important for companies to develop their own cybersecurity policies and an incident response plan to fight against the cybercrimes they eventually are likely to suffer.

Mariana Matos focuses her practice on internal corporate investigations, advising clients on compliance matters, and commercial litigation (with expertise in representing clients in the airline sector). She obtained her law degree from the Pontifícia Universidade Católica – PUC (São Paulo) and a specialization course in compliance from the Fundação Getúlio Vargas – FGV (São Paulo). She is completing a specialization course in Brazilian Civil Procedure (PUC).

.law

Differentiate your firm with
a .law domain.

Exclusive offer for
The Florida Bar members:

[Starting at only \$99/yr]

SECTION SCENE

International Law Section Lunchtime Speaker Series

— 26 April 2017 —

Offices of Fiduciary Trust International Coral Gables, Florida

The International Law Section was pleased to welcome Jeffrey Fisher as the featured speaker for the Lunchtime Speaker Series titled “How to Find \$400 Million.” Mr. Fisher, who is ranked as one of the nation’s Top 10 divorce lawyers, discussed the case of the missing \$400 million that was the subject of a prominent feature story in *The New York Times*. The event was graciously sponsored and hosted by Fiduciary Trust International at its Coral Gables office. Special thanks to Juan Antunez and Adriana Riviere-Badell, members of the Lunchtime Speaker Committee, and Carlos Osorio, ILS secretary, for their work to bring ILS members this outstanding event.



Lunchtime speaker committee members Juan Antunez and Adriana Riviere-Badell with featured speaker Jeffrey Fisher and ILS secretary Carlos Osorio.



Juan Antunez welcomes Jeffrey Fisher to the event.

SECTION SCENE



Participants enjoy a delicious boxed lunch during the ILS Lunchtime Speaker Series.





The Practice Resource Institute

The Florida Bar's most comprehensive resource for running your law practice.

The Florida Bar's Practice Resource Institute is designed to help Florida lawyers with law office operations and to assist members' use of technology. This new digital resource is available on The Florida Bar's website, where members can:



- Live chat with PRI practice management advisors and receive answers in real time.
- Explore comprehensive lists of law office technology, tools, and resources.
- Check out new providers and services in the Bar's Member Benefits program.
- Access shareable electronic tools, web-based archives of articles, blog posts, and podcasts.
- Sign up to be notified of the latest updates.



Technology



Finance



Marketing



New Practice



Management

www.floridabar.org/PRI

Access Wars, from page 13

directly by the government and rather are served on the online service provider, which then has the opportunity to comply with or contest the “warrant.” Under existing case law, a subpoena served on an entity located in the United States can compel that entity to produce records stored abroad so long as the records are in the entity’s custody or control.¹⁰ Microsoft lost its motion to quash the warrant in the lower court, and upon failing to produce the documents stored in Ireland was held in civil contempt, leading to the Second Circuit appeal.

The Second Circuit reversed course, agreeing with Microsoft that the SCA did not apply extraterritorially. It based its decision on the Supreme Court’s “presumption against extraterritoriality,” under which U.S. laws do not apply extraterritorially unless specified by Congress, which Congress did not do with respect to the SCA. Moreover, the court noted that expanding the application of the SCA so it applied extraterritorially would be contrary to the privacy protections for users of online services that it was enacted to create.¹¹

The decision was surprising to many because it cut against the traditional test of “control, not location,” under which the critical element in determining whether a search warrant is executable is whether the entity being served “controlled” the data, as opposed to the location of the data at the time the demand was served.¹² The court, however, distinguished cases that applied that test, noting that they were only applicable to subpoenas and not warrants, and that the types of records subject to those requests were not subject to the heightened privacy protections of the SCA.¹³

This opinion has significant ramifications for U.S. law enforcement investigations in the Second Circuit, and potentially beyond. In the context of criminal investigations, electronic communications providers and other online cloud services receive numerous requests from law enforcement and other government bodies for information they hold about users of their products and services. Indeed, certain Internet companies report receiving an average of more than one and a half requests per minute.¹⁴ As the government pointed out in its briefs in the *Microsoft* case, companies

could potentially frustrate compliance with criminal investigations if they are able to refuse to comply with such requests if the data are stored in a server located overseas.

On the other hand, Microsoft and privacy advocates have trumpeted this case as a victory for individual privacy as well as for comity where the relatively broad authority for law enforcement authorities in the United States to collect information in the context of criminal investigations clashes with stronger individual privacy rights and data transfer restrictions imposed by other countries, particularly in Europe.¹⁵ Indeed, the government of Ireland filed an amicus brief in the *Microsoft* case, formally expressing its concern that the production of data stored on servers located in Ireland had the potential to violate Irish law.¹⁶ Interestingly, the *Microsoft* case occurred during the negotiation of the EU-U.S. Privacy Shield, an important data transfer agreement permitting the transfer of personal information from the EU to certain businesses in the United States when doing so otherwise would be prohibited by EU law. The agreement has its skeptics in Europe who believe that there are too few limits on U.S. law enforcement’s access to commercial data held by companies in the United States, and a ruling against Microsoft might have adversely affected the negotiations, which concluded a couple of months later.

The U.S. government appealed for a rehearing by an en banc panel of the Second Circuit, and in January 2017 was narrowly denied in a 4-4 decision.¹⁷ The U.S. government has not yet petitioned for certiorari to the Supreme Court, but was granted an extension by the court to file such a petition from 24 April to 24 May, an indication that the government is considering filing a petition.¹⁸

In re Google

Subsequent to the Second Circuit’s ruling, the issue of extraterritorial access to data under the SCA has continued to be adjudicated in courts throughout the country, to contrary conclusions.

Access Wars, continued

Just a week after the Second Circuit's denial of an en banc hearing in *Microsoft*, a Pennsylvania federal magistrate judge in *In re Google* denied a motion by Google to quash a request from the government to compel the production of user communications stored overseas, where the information was requested under an SCA warrant.¹⁹ In doing so, the magistrate judge considered and expressly rejected the finding of the Second Circuit in *Microsoft*, which was not binding on the *Google* court.

In distinguishing *Microsoft*, the judge stated that the case should not turn on the extraterritoriality of the SCA, but rather the constitutional review of whether the government's request would constitute a Fourth Amendment "search or seizure," and where that action would take place.²⁰ Considering Fourth Amendment

Therefore, the judge held, the request was essentially a request for data held in the United States, avoiding the question of extraterritoriality.²¹ The judge also distinguished *Microsoft* by pointing to Google's model of "splintering" data across data centers in different countries as frustrating alternative, diplomatic methods of gathering evidence stored overseas, which could not be directed to a single country in order to obtain a full record (see below for an overview of the Mutual Legal Assistance Treaty process).²²

Google appealed this decision on 10 March 2017, and its appeal includes amicus briefs from multiple companies including Amazon, Apple, Cisco, Microsoft, and Yahoo.²³

In re Yahoo

In late February, a Wisconsin federal magistrate judge also aligned himself against the Second Circuit's opinion in *Microsoft* in requiring Yahoo to comply with an SCA warrant for data stored overseas.

In doing so, the judge refused to apply any extraterritorial limitation on the SCA, going so far as to state that orders under the SCA may be termed "warrants" but do not raise privacy concerns that merit the protections typically afforded a search warrant under the Fourth Amendment. He applied the "control, not location" test, and stated that under that test, a request for information stored overseas should be considered as a domestic request would be, so long as the information is within the custody or control of the U.S. recipient.²⁴ He went further to state that "[i]f that service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to



jurisprudence, the judge held that transferring data from servers located overseas to Google in California did not amount to a Fourth Amendment seizure because it did not interfere with account holders' possessory interest in their data, as evidenced by the fact that Google regularly processes such transfers in the course of business.

Access Wars, continued

disclose, consistent with the SCA, that which it can access and deliver within the United States.”²⁵

In the matter of the search of . . . premises owned, maintained, controlled, or operated by Yahoo, Inc.

Even more recently, one judge that had followed the Second Circuit’s reasoning in *Microsoft* reversed course in early April, determining that based on an in-camera reconsideration of its position, the Wisconsin (*Yahoo*) and Pennsylvania (*Google*) cases were more persuasive.²⁶ In considering a different SCA warrant issued to Yahoo, a Florida federal magistrate judge explained that the SCA gives the court in personam jurisdiction over the electronic communications service, agreeing that an SCA warrant is more like a subpoena than a traditional warrant.²⁷ He also questioned whether electronic data constitutes tangible property as contemplated by a search warrant, and held that the restrictions on access within the SCA were adequate to balance any privacy concerns.²⁸

Are Multiple Legal Assistance Treaties a Viable Alternative?

In *Microsoft* and similar cases, the U.S. government has argued that if it is unable to require U.S. cloud service providers subject to the SCA to produce data stored on overseas servers, companies will be incentivized to store such data overseas and frustrate law enforcement objectives. Technology companies and privacy advocates, on the other hand, have argued that there is a viable method already in place: Mutual Legal Assistance Treaties (MLATs).

MLATs are bilateral or multilateral treaties between countries through which, among other things, the parties agree to collect and share evidence of certain crimes or other violations of law, subject to a variety of restrictions.²⁹ The United States alone has more than fifty-five bilateral MLATs in place, in addition to a multilateral agreement with the EU member states that was reached in 2010.³⁰ Figure 1 shows current MLATs, an



Figure 1: Current MLATs (image from mlat.info, licensed under Creative Commons, attributable to Access Now)

impressive array of agreements that span much of the globe.

In the cases outlined above, technology companies have argued that instead of violating principles of extraterritoriality by forcing the companies to produce data stored overseas, potentially in violation of foreign law, the U.S. government should instead submit a request under its MLAT with the other country for law enforcement to collect and provide the information.

The U.S. government, however, has resisted relying on this approach, as the process for requesting an MLAT is time-consuming and difficult.³¹ A recent estimate put the time needed to fulfill an MLAT request, from diplomatic contact to receipt of information, at an average of ten months.³² The U.S. government has argued that a ten-month delay in receiving evidence is simply too long, especially when such information is often critical to a criminal investigation with U.S. victims. Moreover, MLATs are riddled with exceptions, allowing countries to decline to produce evidence where enforcing the law being investigated would run contrary to the laws and values of the country asked to produce the evidence. For example, the United States could decline under its MLATs to produce information needed to support the investigation of a speech-based crime in another country, if that speech is protected in the United States under the First Amendment.

While the MLAT process is much the same as it was when the United States signed its first MLAT with Switzerland in 1977, the costs of storing and transporting data have plummeted. This increases the likelihood that evidence relating to local crimes, which was traditionally stored and accessible within the United States, will

Access Wars, continued

be stored abroad, thus invoking the complex MLAT process. For example, if a suspected criminal in the United States stores documents potentially relevant to an investigation with a U.S.-based cloud provider, it is quite possible that the cloud provider stores those documents on a server farm outside of the United States due to cost, convenience, compliance obligations, or a variety of other reasons (even without the knowledge of the suspected criminal). Forty years ago, that information likely would be stored on site or in filing cabinets, making it easier for local law enforcement to access.

Indeed, the government argues that the effect of the byzantine nature of extraterritorial requests for data stored abroad and the complexity of the MLAT is to help criminals avoid prosecution. There is even the possibility that sophisticated criminals might attempt to frustrate law enforcement by using foreign privacy laws to a similar effect as tax shelters.

One thing is certain; the proliferation of requests for data by law enforcement is rising quickly.³³ Just as the Internet has shifted traditional notions of data “residence,” it has also increased the interest that global governments have in data. Protectionist governments may, for example, use data requests to seek to exercise their sovereignty, to promote their global data standards (perhaps as a means to prop up their technology sectors), or to obtain data from companies to advance economic or intelligence interests. For example, we have seen this in Russia, which in 2014 enacted a data localization law that requires companies collecting personal information in Russia to store a local copy within the territory of Russia.³⁴

It is clear that governments view MLATs as insufficient to meet the demands of modern investigation where evidence is stored with third-party cloud service providers, and diplomatic efforts are underway to improve the efficiency of the MLAT process. For example, some have suggested that the MLAT process be streamlined for certain trusted partner countries, analogous to the visa waiver process in the immigration system.³⁵ Likewise, a U.S.-UK government data request

agreement is under negotiation that could be a prototype for developing procedural elements in future agreements.³⁶

If the Second Circuit’s opinion in *Microsoft* becomes the law of the land—which is looking less likely, given the contrary lower court cases—the U.S. government will be deprived of one of its key methods of collecting information stored abroad outside of the MLAT process, which could accelerate diplomatic efforts or congressional action to amend the territorial scope of the SCA.

U.S. Congressional Action

The Electronic Communications Privacy Act (which includes the SCA) was passed in 1986 at a time when the Internet was in its nascent stages, and there is near-uniform recognition that it needs to be amended to respond to modern considerations. Many, including the court in *Microsoft*, have argued that the courts are a less than ideal venue to determine the intent of lawmakers from over thirty years ago in applications that were unforeseeable at the time. Just last year, the U.S. House of Representatives passed a reform bill (the Email Privacy Act) by a rare unanimous roll-call vote.³⁷ Among several important provisions in that bill was the inclusion of an administration proposal to authorize bilateral agreements to facilitate government requests for data—a type of streamlined MLAT process.³⁸ The bill, however, was never voted on in the Senate.

This January the Email Privacy Act was reintroduced, but there are concerns that relevant committees will be occupied with reauthorization of the Foreign Intelligence Surveillance Act (FISA) Courts, which will sunset at the end of 2017.³⁹

U.S. Rules of Criminal Procedure

Another recent and relevant development related to U.S. courts’ extraterritorial access to data was a change to the rules that govern criminal prosecutions, the Federal Rules of Criminal Procedure (FRCP). In December 2016, the Judicial Conference of the United States changed

Access Wars, continued

Rule 41 of the FRCP so that a federal judge can now grant a warrant to remotely access, search, and seize data located anywhere in the world if the location of that data is concealed through electronic means, or appears to be a part of an infected network (otherwise known as a “botnet”).⁴⁰ Consumers located abroad who use tools that protect the privacy of their location would be subject to these searches, as would consumers located abroad who are unknowingly infected by botnets.⁴¹ Both of these expansions to access fail to account for the location of the data, sidestepping the MLAT process. It should also be noted that for certain criminal enterprises, Section 32B of the Cybercrime Convention has allowed for signatories (including the United States) to access data outside of the MLAT process in limited circumstances.⁴²

Conclusion

Given the divergent results among the jurisdictions that have considered how requests for extraterritorial data should be handled and the fact that leading technology companies tend to be globally integrated, the resolution of these questions will become increasingly important. To be sure, law enforcement agencies and regulators will continue to seek data relevant to criminal investigations through various means, regardless of the locality of that data. It remains an open question whether judicial decisions, congressional action, or more efficient global law enforcement cooperation will move the needle toward a common standard. Also, public opinion and consumer advocacy have and will continue to play a role in companies' actions.

The net result of this uncertain landscape is that for the time being, law enforcement and companies may have to continue to apply multiple standards to law enforcement requests. Even if *Microsoft* is overturned, it is uncertain how other governments will react, and they could increasingly seek to apply their standards globally as well. This war of conflicting standards would not benefit anyone, except, perhaps, authoritarian countries that seek to use global technology companies as a branch of their intelligence services or protectionist

countries that seek to force global technology companies to localize their data.



Bret S. Cohen is a partner in Hogan Lovells US LLP. With a particular focus on the Internet and e-commerce, he has advised extensively on legal issues related to cloud computing, social media, mobile applications, online tracking/analytics, and software development. He counsels and is a frequent speaker on strategic compliance with global privacy laws, including cross-border transfer restrictions, data localization requirements, and the impact of government surveillance on the digital economy.



Lillian S. Hardy is a partner in Hogan Lovells US LLP. She focuses her practice on Foreign Corrupt Practices Act (FCPA) investigations, economic sanctions, cybersecurity and data privacy-related investigations, consumer financial protection enforcement actions, and other government investigations. She has managed wide-ranging investigations for clients on five continents and works with companies to develop and improve their compliance programs.



Charlie Wood is an associate with Hogan Lovells US LLP. He joined the global privacy and cybersecurity practice after working on privacy and cybersecurity issues at a leading social media company, the White House, and the U.S. Senate. His interests and experience span consumer privacy, national security, fin tech, and ad tech, with a focus on innovative products and services. He is only admitted to practice in California; he is supervised by principals of the firm.

Access Wars, continued

Endnotes

- 1 See generally, *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016).
- 2 See, e.g., *Smith v. Maryland*, 442 U.S. 735 (1979).
- 3 18 U.S.C. § 2703.
- 4 *Id.* §§ 2703(a), (b)(1)(A).
- 5 *Id.* §§ 2703(b)(1)(B), (c), (d).
- 6 *Id.* § 2703(g).
- 7 See *id.* at 197.
- 8 See *id.* at 222.
- 9 See *id.*
- 10 See *id.* at 197, citing *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983).
- 11 See *id.* at 219.
- 12 See *In the Matter of a Grand Jury Subpoena Directed to Marc Rich & Co. v. United States*, 707 F.2d 663, 667 (1983).
- 13 See *id.* at 215-6.
- 14 See *Google Transparency Report*, Google, <https://www.google.com/transparencyreport/removals/government/> (last visited 3 April 2017), indicating they received more than 400,000 requests in the second half of 2015, or 1.52 requests per minute.
- 15 See Brad Smith, *Our search warrant case: An important decision for people everywhere*, Microsoft Blog (14 July 2016), <https://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#P5i4f33FPEohPswc.99> (last accessed 17 April 2017).
- 16 See Mark Scott, *Ireland lends Support to Microsoft in Email Privacy Case*, (24 December 2014), https://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/?_r=0.
- 17 See Jane Metcalf & Harry Sandick, *Sharply Divided Circuit Denies Government's En Banc Petition in Microsoft Appeal*, *supra*.
- 18 See The Supreme Court of the United States Docket File 16a927 (12 April 2017), <https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles\16a972.htm> (last visited 17 April 2017).
- 19 See *In re Search Warrant No. 16-960-M-01*, 2017 WL 471564, at *1.
- 20 See Orin Kerr, *Google Must Turn Over Foreign-Stored Emails Pursuant to a Warrant, Court Rules*, Washington Post (3 February 2017), https://www.washingtonpost.com/news/voikh-conspiracy/wp/2017/02/03/google-must-turn-over-foreign-stored-emails-pursuant-to-a-warrant-court-rules/?utm_medium=twitter&utm_source=dlvr.it&utm_term=.41855a140d05.
- 21 See *In re Search Warrant No. 16-960-M-01*, 2017 WL 471564, at *9.
- 22 See *id.* at *13-14.
- 23 See *Microsoft Corp, Amazon.com, Cisco Sys., Inc. & Apple Inc. Amicus Brief*, Misc. Nos. 16-960-M-1, 16-1061-M (E.D. Pa. 10 March 2017); *Yahoo, Inc. Amicus Brief*, Nos. 16-960-M-1, 16-1061-M (E.D. Pa. 10 March 2017).
- 24 See *In re Search Warrant No. 16-960-M-01*, 2017 WL 471564, at *5.
- 25 See *In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo*, 2017 U.S. Dist. Lexis 24591, at *7.
- 26 See [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., No. 17-mj-1238, Order (M.D. Fla. 10 April 2017)

27 See *id.*

28 See *id.*

29 In the absence of a treaty, countries use letters rogatory, a lesser used mechanism not detailed in this article. Notable exceptions include the U.S. government's use of a letter of rogatory to Iceland in the Silk Road investigation and the French government's use of letters of rogatory in the wake of the Charlie Hebdo attack. More on letters of rogatory can be found here at *Preparation of Letters Rogatory*, U.S. Department of State, Legal Consideration, <https://travel.state.gov/content/travel/en/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.html> (last visited 3 April 2017).

30 See Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, Georgia Tech Scheller College of Business Research Paper, No. WP 38, pp. 12-13 (11 January 2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

31 See Peter Swire & Justin D. Hemmings, *supra*, pp. 12-16.

32 See *Liberty and Security in a Changing World*, National Archives and Records Administration, p. 227, available at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last visited 3 April 2017).

33 See *Government Request Report*, Facebook, <https://govtrequests.facebook.com/> (last visited 3 April 2017); *Google Transparency Report*, *supra*.

34 See Bret Cohen, Natalia Gulaeva, and Maria Sedykh, *Russia Update: Regulator Publishes Data Localization Clarifications* (11 August 2015), <http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications> (last visited 17 April 2017).

35 Peter Swire & Justin D. Hemmings, *supra*, pp. 45-51.

36 See Ellen Nahashima & Andrea Peterson, *The British Want To Come To America — With Wiretap Orders And Search Warrants*, Washington Post: National Security (4 February 2017), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html?utm_term=.7f069e69c3df.

37 See *ECPA Reform*, Center for Democracy & Technology: Security Surveillance, <https://cdt.org/issue/security-surveillance/ecpa-reform/> (last visited 3 April 2017).

38 See Letter from Peter J. Kadzik, Assistant Attorney General, U.S. Dep't of Justice to Honorable Joseph R. Biden, p.4 (15 July 2016), <https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document>.

39 See Caroline Lynch, *ECPA Reform 2.0: Previewing the Debate in the 115th Congress*, Lawfare: Surveillance (30 January 2017), <https://www.lawfareblog.com/ecpa-reform-20-previewing-debate-115th-congress>.

40 See *Proposed Fed. R. Crim. P. 41*, Just Security (16 September 2014), available at <https://www.justsecurity.org/wp-content/uploads/2014/09/proposed-amendment-rule-41.pdf>.

41 See Rainey Reitman, *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to Government*, Electronic Frontier Foundation: Deeplinks Blog (30 April 2016), <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government>.

42 See Stanford Center for Internet and Society, *Law Enforcement Access to User Data, Law, Borders, and Speech Conference*, YouTube (24 October 2016), <https://www.youtube.com/watch?v=YU-LtW5SO3c>.

Hacking Back, from page 15

forensics, investigations, legal supervision, and crisis communication advice. These pre-vetted organizations are often made available at discounted rates to companies hit with breaches. They are available quickly, which is important because knowing what happened may be key to assuring that the leakage has been stopped, and there may be governmentally imposed reporting deadlines that must be met. Where payment card information is compromised, the affected banks may want the investigation carried out by a preferred forensic investigator (PFI) that has been approved by the payment card industry's security council to conduct such investigations.

In carrying out the investigation, the insurer may determine that knowing the identity or even the type of organization that carried out the attack is not something it needs or wishes to pay for. In these cases, a company must determine if there is a justification to spend potentially significant funds that will not be reimbursed by the insurer to determine who conducted the attack.

Get our data back—or destroy our data that the crooks are holding! And punish them if you can!

We have seen many executives call their technology units to demand quick action to retrieve stolen data from perpetrators, or to somehow remotely destroy it, so that the criminals cannot exploit it. We've also seen executives ask their IT staff whether they can retaliate, saying things like "they hacked us, why can't we hack them?" or "can you knock them off of the Internet?"

Those sentiments are understandable. The company has been attacked and hurt. Remediation may cost millions of unbudgeted dollars/euros/pounds, etc. There may be reputational damage that ultimately costs far more than the monetary expenditures. Add to this the reality that law enforcement authorities may not be able to touch the perpetrators. They may not be able to attribute with the level of knowledge and evidence needed to sustain a conviction. The evidence may not even be strong enough to sustain a civil judgment (assuming you can find a court to hear the case given the usual difficulties in determining absolute attribution). Do-it-yourself

retribution—often called *hacking back*—may make a company's executives feel good, but analysis indicates many reasons why ultimately, whether the actions are successful or unsuccessful, they are, for private-sector organizations, almost universally a bad idea.

Consider the following do-it-yourself hack-back scenario. A company we will call Peterson Recreation and Occupational Center (PROC) suffers a data breach. Its internal IT department executes its incident response plan. Examination of computer server logs reveals that sensitive data was stolen by the perpetrators. In fact, the IT investigators have determined that the data was moved to a specific server at a specific IP address. Following instructions from management to go after the perpetrators, the IT department gets into the server and sees a folder called PROC_DATA. The IT people believe that because of the folder's name, it is PROC's stolen data. Upon looking in the folder, they find that they can't read the file because it appears to be in a format they're not familiar with. "Perhaps," they report, "it's in an encrypted archive." Management asks them what they can do. They decide to buy a "ransomware toolkit" on the Internet and use it to encrypt the hard drive of the target machine. They are careful to set up the ransomware so it will not spread to other computers. And of course they put fake information into the part of the ransomware that tells the victim of the malware how to pay to get their data back. They do this because they have no interest in or intention of providing a decryption key.

Meanwhile, the National Center for Pediatric Oncology—a leading hospital treating childhood cancers located in a different country than Peterson—doesn't know that hackers from another continent have compromised one of its servers and are using part of that server's storage as an intermediate holding site for data stolen by the hackers from victims in at least ten countries.

One day, without warning, the hospital's CEO gets a call from the IT security group. One of the hospital's servers has been hit with ransomware. All of the data on the hard drive is now encrypted. The ransomware screen demands a payment of 1 bitcoin to regain access to the

Hacking Back, continued

files, but the contact information (should the hospital want to make the ransom payment) is gibberish. Bottom line: the data is gone. The CEO asks what data was on the server. She is told that a lot of it was software that can easily be replaced, but there was a key directory called "PROC_DATA." Here, PROC stands for Pediatric Radiation Oncology Computer, and each subfolder holds both the settings for the radiation therapy machines used to treat a specific patient and the records of the actual treatments. Unfortunately, the backups are stored on a different part of the hard drive, and they, too, are encrypted.



The pediatric hospital calls the cybersquad of the federal police, which launches an immediate criminal investigation. The hospital informs its cyberinsurance carrier, which authorizes the hospital to execute its incident response policy and approves an initial expenditure of 100,000 euros. Forensic experts, investigators, a crisis communication company, and specialized legal resources are immediately engaged. A data recovery company is engaged to try to decrypt the files (ultimately unsuccessfully).

The investigators are able to trace the intrusion back to the Peterson Recreation and Occupational Center. (It turns out the vigilante hack-back team members weren't masterminds when it came to hiding their tracks.) The hospital's counsel informs PROC that he has proof that PROC attacked the hospital, installed malware, and destroyed data that was critical to treating children who have life-threatening cancers.

Consider the problems now facing PROC, which shortly before this had been rejoicing in the success of its hack-back project.

- PROC's actions violated the laws of its home country. Peterson intruded into a computer without authority.

It deliberately infected the computer with malware, knowing the damage it would do. The malware committed extortion by seeking a ransom payment.

- PROC's actions violated the laws of the country in which the hospital operates. PROC has committed clear cybercrimes, and the federal authorities in that country have decided to press charges and seek extradition under a bilateral treaty between the home countries of Peterson and the hospital.
- The hospital and its insurer engaged counsel in Peterson's country and filed notice that they are lodging a civil suit seeking recompense for their costs, plus punitive damages.
- Even worse, the hospital called a news conference jointly with its national justice ministry and national police cyberexperts. A pediatric radiation oncologist explained how the hack back impeded the hospital's treatments of seriously ill children. Several parents of patients who could not get their radiation therapy treatments also spoke. Peterson is now suffering incredible reputational damage for its actions that put the lives of children who have cancer in danger.

All of this goes to prove that hacking back is not something that one can do without consequences. Last

Hacking Back, continued

year, there was a proposal to authorize U.S. companies to conduct limited hack-back operations (with the understanding that they were not to damage networks or data) and to immunize them against charges under U.S. law. Obviously, U.S. legislation cannot immunize a company against the laws of other nations that may well see a hack back as an attack. Further, even if the incident only involves U.S.-based systems, it seems unjust that the victim of the hack back should have to pay the costs of the incident response (which can be significant even if data is not destroyed) or that the insurer should bear such costs. Failure to consider either the civil remedies available to the hack-back victim or the reputational damage that can be heaped on the company doing the hack back doesn't mean these consequences won't happen. For the company that hacks back, the "law of unintended consequences" may come into play. While a company may rely on a law that immunizes it from criminal liability, it might fail to consider the potential for civil court action or reputational damage.

How can a company avoid the problems that can follow even the most successful hack-back attack?

The most obvious answer is the simplest: don't do it! Because some individuals within a company may think that hacking back is a good idea, the best defense is to have a process in place that involves making the company's counsel a key part of the decision-making structure. No hacking back should be permitted without the consent of counsel, who presumably is in a position to warn the company of the kinds of criminal, civil, and reputational downsides to such actions. The risk manager can be another source to reference. The risk manager probably has already notified the carrier of the company's cyberinsurance coverage, and may, at the insurer's request and working with corporate counsel, engage a law firm specializing in data breach response (sometimes called a "breach coach"). Such coaches play an important role, in that an average corporate attorney will have very limited experience in dealing with cyberbreaches, whereas a breach coach does it all the time.

Ultimately, decisions to take hack-back actions are made

by senior management. But those decisions can have far-reaching consequences. Company employees may find themselves under arrest or named in civil suits. Company representatives in countries hit by the hack back may be detained, and company operations in that country may be adversely affected or even halted.

The potential problems associated with private-sector hack back, given the diversity of laws concerning cybercrime and the likelihood of civil action and reputational damage, should dissuade companies from thinking like cybervigilantes. Counsel, we believe, should play an integral part in making sure that those favoring a hack-back solution understand the consequences, both to the company and to themselves as individuals.



Alan Brill is senior managing director and founder of Kroll's cyberpractice. He is an internationally known expert on cyberinvestigations and cybercrime. Prior to joining Kroll, he was a director in the New York City Department of Investigation and deputy inspector general

in New York. He was a major in the U.S. Army, assigned to the Office of the Secretary of Defense, and worked with the NASA Manned Spacecraft Center in Houston during the Apollo moon landing project. He is an adjunct professor at the Texas A & M University School of Law.



Jason Smolanoff is a senior managing director and global head of Kroll's cybersecurity and investigations practice. He served as a supervisory special agent of a cyber national security squad in the U.S. Federal Bureau of Investigation's Los Angeles field office. He is an

adjunct professor at Loyola Law School, Los Angeles, where he teaches incident response and investigations.

Endnotes

- 1 *Spokeo, Inc. v. Robins*, 578 U.S. ____ (2016).
- 2 *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 560–561, at 560. Pp. 7–11.

International Data Privacy, from page 17

Where in the World Is George Que?

This article will discuss the primary data privacy laws implicated in the context of the following scenario³:

ABC Co., a U.S. company, sends its executive employee, George Que, on an extended business trip during which he is expected to spend several months working in Canada, the United Kingdom, Germany, Japan, and Australia. ABC Co. does not have any foreign affiliates. The ABC Co. employee handbook contains an electronic communications policy that provides, in relevant part:

Electronic communications include all aspects of voice, video, and data communications, such as voice mail, email, text, fax, smartphone, and Internet access. All information, data, and messages created, received, sent, or stored in these systems are, at all times, the property of the Company and are monitored continuously by the Company. You are required to use your access for business-related purposes (e.g., to communicate with customers). However, personal use of the company's electronic communication tools is permitted, so long as such use is reasonable and does not otherwise interfere with legitimate business uses. For business purposes, management reserves the right to search and/or monitor the company's Internet usage and the electronic communications, files, and/or transmissions of any employee without advance notice and consistent with applicable state and federal laws. Employees should expect that the electronic communications that they send and receive will be reviewed and disclosed to management. Employees should not assume that the electronic communications that they send and receive are private or confidential. Any electronic communications that violate company policy can lead to disciplinary action, up to and including termination of employment.

Pursuant to its policy, ABC Co. continuously monitors all employee emails in furtherance of its legitimate business interests in evaluating employee performance, proactively monitoring for potential legal violations committed by employees and conducting quality assurance reviews to improve customer service. When ABC Co. carries out an internal investigation based on an employee complaint, an ethics hotline complaint, or a manager's suspicion of an employee's lack of productivity, ABC Co. accesses and reviews employee-generated emails archived in its network.

George is aware of ABC Co.'s policy and has signed an

acknowledgment form confirming that he received and reviewed the employee handbook containing this description of the scope of ABC Co.'s email monitoring activities. Because George travels regularly, he uses his company-issued laptop for both business and personal use. In the ten years George has worked for ABC Co., the company has never received any complaints of wrongdoing against him and has never conducted an internal investigation during which George's emails were reviewed. Indeed, George was chosen for this international assignment because of his exemplary work record. While George is working remotely and using his company-issued laptop during this international assignment, however, several issues arise that lead ABC Co. to access and review George's emails.

Will ABC Co.'s Policy Pass Muster With Our Neighbors to the North?

George begins his multinational business trip in Canada. He is in the second month of his three-month assignment in Canada when ABC Co. receives an anonymous phone call reporting that George has been revealing confidential and proprietary ABC Co. information to its competitors. ABC Co.'s chief executive officer gives the directive to launch an immediate investigation into these allegations, including the search and review of George's emails. Should ABC Co. rely on U.S. law and conduct the search, or should it look to Canadian law?

While recognizing a privacy interest for employees to a greater extent than the United States, Canada's approach to privacy protection is still developing. Canada's main privacy law is the Personal Information Protection and Electronic Documents Act. This statute regulates the protection of the personally identifiable and personal health information that an employer collects, maintains, and discloses about its employees.⁴ It does not appear to govern an employer's ability to internally monitor an employee's emails on company-owned systems.

Canadian case law acknowledges that employees may have a privacy interest in their personal information contained on their employer-owned computers. Canadian courts consider the ownership of the computer

International Data Privacy, continued

system and the employer's workplace policies as relevant factors in deciding whether the employee has a reasonable expectation of privacy, but they are not determinative.⁵ The courts use a totality of the circumstances test "in order to determine whether privacy is a reasonable expectation in the particular situation."⁶ Thus, Canadian law balances the employee's privacy interests, the employer's legitimate business interests in monitoring its employee's emails, and the practices or circumstances within the specific workplace at issue. The relevant practices and circumstances include the wording of the employer's policies, the enforcement of those policies, and the employee's ability to use the employer's computer system for personal use.

In our scenario, it is unlikely that Canadian law would apply, given that George is not a Canadian citizen and ABC Co.'s operations are solely in the United States. It is possible, however, that Canadian law would apply if the facts in the scenario were slightly different. For example, if an ABC Co. employee was spending a sufficient amount of time living and working in Canada that he could be considered a Canadian national, or at least needed a Canadian work visa, then Canadian law would be more likely to apply. Of course, if ABC Co. had hired a Canadian citizen who was working for ABC Co. remotely in Canada, then Canadian law would apply. In George's case, the issue is most likely determined by the extent of the connections that can be established between Canada and the conduct at issue.

Assuming that Canadian law applies, or if, in an abundance of caution, ABC Co. elects to follow Canadian law, ABC Co. must balance its interests in searching the emails with George's privacy interests in any personal communications he created or personal data contained in his emails. George is aware that ABC



"We'll never guess her password."

Co. monitors its employees' emails. Its policy states that employees' communications on employer-owned systems, whether business or personal, are subject to search by management and that the content of electronic communications could lead to the company taking disciplinary action against employees. ABC Co. also has a legitimate interest in searching George's email to investigate the allegations of theft of trade secrets made against him. Accordingly, the totality of the circumstances analysis weighs in favor of ABC Co., and leads to the conclusion that George should not have a reasonable expectation of privacy in his emails and that ABC Co. should be able to search those emails without violating Canadian law.

International Data Privacy, continued

Can ABC Co. Monitor George's Emails From Across the Pond?

Fortunately for George, the investigation showed that the allegations against him were baseless, and he has continued on to the next stop on his assignment, the United Kingdom. Life is good for him traveling throughout the UK, and he has been very productive in his work assignments there. Two and a half months into George's UK assignment, however, his assistant, Lola, has complained to ABC Co.'s human resources director that George made sexual comments to her at a dinner meeting with other coworkers before he left for Canada; emailed sexually based jokes to her; and called and emailed her frequently to ask her what she was wearing and to ask her to "talk dirty" to him. Upon receiving Lola's complaint, the human resources director launched an investigation into the allegations. In addition to conducting witness interviews, the human resources director has also asked the head of information technology to collect for review all of the emails in ABC Co.'s network between George and Lola. Will the law of the United Kingdom affect ABC Co.'s ability to legally conduct its email review as part of the investigation into Lola's sexual harassment complaint?

Pursuant to the Regulation of Investigatory Powers Act of 2000 (RIPA), employers in the United Kingdom⁷ are required to obtain an employee's actual or constructive consent prior to intercepting and monitoring the employee's emails generated and maintained on the employer's computer systems.⁸ When intercepting and monitoring these emails, the employer must have a reasonable belief that both the employee and the recipient of the email have consented (implicitly or explicitly) to its interception.⁹ Thus, where an employer has a clear policy, acknowledged by the employee, the employer should be able to establish that the employee consent requirement has been satisfied. The policy should provide that the employee has no expectation of privacy when using the employer's computer systems and that the employer is intercepting and monitoring all emails generated on the employer's system. The element of the test that will be more difficult for the

employer to demonstrate is that the recipient of the communication consented to its interception and monitoring. The law applies to any "person" who is intercepting communications "at any place in the United Kingdom."¹⁰

In addition, the Data Protection Act of 1998 (DPA) applies to the monitoring of employee emails.¹¹ While the DPA does not prevent employers from monitoring an employee's emails, "it sets out principles for the gathering and use of personal information. In short, data protection means that if monitoring has any adverse effect on workers, this must be justified by its benefit to the employer or others."¹² The DPA requires transparency or "openness." Like the RIPA, the DPA requires a clear policy or notice of the reasons for the email monitoring and the types of monitoring that will take place.¹³

Whether UK law would apply to ABC Co. depends on how its monitoring of employee emails is conducted. If the emails are being transferred or collected from a location in the UK, then the law would apply. Accordingly, the RIPA and the DPA would likely apply to emails that George generated in the UK. Turning then to the application of those laws, the fact that ABC Co. had an electronic communications policy and George was aware of that policy would weigh in favor of ABC Co.'s ability to monitor and review George's emails. ABC Co.'s policy, however, is not as transparent as UK law requires, as it does not state the methods ABC Co. uses to monitor the emails and the specific legitimate business reasons for which ABC Co. conducts the monitoring. Based on this, ABC Co.'s plan to collect and review George's emails would be inconsistent with UK law. In addition, some best practices that ABC Co. should consider going forward is to obtain informed, written consent from its employees before they travel to the UK, and to have the information technology department include a message on all of the employees' outgoing emails stating that those emails are being recorded and monitored by ABC Co., in order to give the recipient the notice required by the RIPA.

International Data Privacy, continued

Full Speed Ahead With Email Monitoring on the Autobahn?

While Lola's complaint was being investigated by ABC Co., George completed his assignment in the UK and traveled to Germany to continue his work for the company. The human resources director wants to obtain a copy of the hard drive from George's laptop in order to examine any data he may have surreptitiously saved there instead of to the company's network. Does German law affect ABC Co.'s ability to inspect the hard drive?

In Germany, employee email monitoring is governed by the Federal Data Protection Act,¹⁴ which applies when a company collects, processes, or uses personal data in Germany or if a German branch of the company carries out the collection, process, or use.¹⁵ Whether an employer can monitor its employee's emails depends largely upon whether the employer allows the employee to use its computer system for personal use, in addition to business purposes.¹⁶ Where an employer permits such dual use, the employee has a privacy interest in the emails and the employer cannot monitor any of the emails, including the business communications, unless the employer can show that the monitoring is necessary for the maintenance of the email system and serves

the collection purposes for which the email system was established,¹⁷ or that the employee has freely provided written consent after being "informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent."¹⁸

Employers may collect, process, or use an employee's personal data without the employee's consent for employment-related purposes when it is necessary in making hiring decisions, or after an employee is hired for "carrying out or terminating the employment contract." The data may also be used without the employee's consent when it is necessary to investigate an employee-committed crime, provided that the employer has a documented reason to believe the employee committed a crime while employed by the company and the privacy rights of the employee do not outweigh the need to investigate the alleged crime.¹⁹

Germany's data protection scheme is problematic for ABC Co. Because ABC Co. permits dual use of its computer system, George has a privacy interest in the emails on his work-issued devices. It is unlikely that ABC Co. can establish that the monitoring, and even more so the review of George's emails, is necessary as part of

NEED TO UPDATE YOUR ADDRESS?

The Florida Bar's website (www.FLORIDABAR.org) offers members the ability to update their address and/or other member information.

The online form can be found on the website under "Member Profile."



International Data Privacy, continued

ABC Co.'s maintenance of its email system and serves the collection purposes for which the email system was put in place, which was likely for the creation of business records and for employees to conduct company business, rather than for investigation of alleged employee misconduct.

The consent exception may not be a route available to ABC Co., either. At this stage of its investigation, ABC Co. may not want George to know about the complaint Lola has made about him and may not want to tell him that it is seeking to collect and review his emails as part of an investigation into alleged misconduct by him. Even if ABC Co. is willing to advise George of the complaint and ask for his consent to collect and review his emails, George may not consent. If George agrees to ABC Co.'s request, ABC Co. will want to prepare a written consent form for him to sign that makes clear that George is freely providing his consent and is not consenting simply because he fears he will otherwise suffer an adverse employment action. If, as a result of the review of George's emails, ABC Co. finds a basis to conclude that he acted inappropriately and it suspends or terminates him, George may challenge the legality of the review and the validity of the consent he gave, arguing that ABC Co.'s request for his consent was inherently coercive and that he believed he could not refuse without jeopardizing his employment with ABC Co.

The options available to ABC Co. if it wants to proceed with the collection and review of George's emails, either without seeking his consent or after he refuses to consent, are slightly better for the company, but by no means a slam dunk. The crime exception is inapplicable in the present situation because the allegations against George do not rise to the level of a crime. ABC Co. has a stronger argument that it is seeking to collect and review George's emails for employment-related purposes. Those purposes would include carrying out its obligations under its employment relationship with George, which, it would argue, include ensuring that George is not violating company policy or the U.S. civil statutes prohibiting sexual harassment and the creation of a hostile work environment; complying with its duty to

supervise George; and preventing a potential negligent supervision claim by people who work with George, both in the United States and during his international business trip. While ABC Co. can make this argument under the Federal Data Protection Act, German law complicates ABC Co.'s plans to collect and review George's emails.

Does George's Next Stop Include Sushi, Sake, and Surveillance?

ABC Co. decided it did not want to risk compliance issues in Germany, so the company cut short George's assignment there and sent him to Japan. The human resources director wants a Japanese company to copy George's hard drive and send it back to her in the United States so that she and the information technology director can review its contents as part of the investigation into Lola's complaint.

The Japanese Act on the Protection of Personal Information protects against the unauthorized disclosure of personal information of Japanese citizens or foreign nationals, defined as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information."²⁰ The main purpose of the Act is to require the protection of the personal information by governing the manner in which an entity handles the information while balancing the privacy interests of the individual and the "usefulness of the personal information."²¹ The Act does not appear to regulate an employer's internal monitoring of employee emails. Legal commenters on Japanese law have opined that as long as the employer owns the computer system and provides notice of the monitoring, the purpose for which the monitoring is conducted and that disciplinary action could result from the monitoring, the employer does not need the employee's consent in order to monitor emails that are generated and saved on the employer's computer system.²²

Japanese law would likely not apply to the search of George's hard drive because George is neither a Japanese citizen nor a foreign national. Accordingly, it does not prevent ABC Co. from proceeding with its plan

International Data Privacy, continued

to copy and review the contents of the hard drive on George's company-issued computer. If the law did apply, it could provide an obstacle for ABC Co.'s plan to copy and search George's hard drive unless George consents. While ABC Co. has an electronic communications policy, and George is aware of that policy, the policy arguably does not satisfy the requirements of the Act, which require that the policy state the purpose for which the monitoring is being conducted.

Will ABC Co.'s Monitoring Policy Stand Up to the Laws of the Land Down Under?

Although ABC Co.'s investigation was inconclusive, it reassigned Lola to work for a different executive and required George to undergo an online sensitivity training course. George completed that course while he was in Australia, where ABC Co. had sent him to work on a project that arose unexpectedly while he was in Germany. The human resources director has remained wary of George and has instructed the information technology director to monitor George's emails and to let her know immediately if he finds any "suspicious or troublesome" activity. Will Australian law affect this directive?

Australia's privacy law has two components: (1) the Privacy Act of 1998 (Privacy Act), which includes thirteen Australian Privacy Principles (APP); and (2) an amendment to the Privacy Act (governing private organizations), entitled the Commonwealth Privacy Amendment (Private Sector) Act 2000.²³ In pertinent part, the APP requires transparency in the management of personal information, including the publication of a privacy policy informing individuals about the purposes for, and processes by which, the company collects, stores, uses, and discloses personal information.²⁴ While the APP requires this general privacy policy, the Commonwealth Privacy Amendment, which regulates the collection, use, and disclosure of personal information, contains an exemption for "employee records."²⁵ In order for the employee records exemption to apply, the employee must be a current or former employee of the company, and the record must be

held by the company as a result of the employment relationship.²⁶ Employee emails generated as part of the employment relationship may be considered employee records depending on the content of the emails and whether they contain personal data.²⁷

Individual states within Australia have enacted their own laws to regulate the monitoring of employee workplace computer use. For example, the New South Wales Workplace Surveillance Act of 2005 (NSWWSA) regulates employer surveillance of employees, which includes monitoring of employee emails on the employer's premises, the premises of a related corporation, or any other place where the employee performs work for the employer. The NSWWSA requires employers in Sydney, and other cities in New South Wales, to provide written notice of monitoring to an employee at least fourteen days in advance of the start of the monitoring, and permits the employee to agree to a shorter notice period. If employee monitoring is already in place when an employee is hired, then the notice must be provided before the employee starts work.²⁸ The notice must be in writing and acknowledged by the employee in such a manner that "it is reasonable to assume that the employee is aware of and understands the policy."²⁹ Employers who wish to carry out "covert surveillance," that is, the monitoring of an employee at work without notice for the purpose of establishing whether the employee is involved in unlawful activity, must obtain authorization from a magistrate judge to do so.³⁰

Similarly, the Australian Capital Territory Workplace Privacy Act 2011 requires employers to provide advance notice of employee monitoring to employees in Canberra and other places within the Capital Territory, and prescribes the contents of the notice.³¹ Where a state within Australia does not have a law addressing email monitoring, employers can look to the requirements of the country laws discussed above for guidance.³²

While seemingly more favorable to ABC Co. than German law, Australian law also presents roadblocks to ABC Co.'s plan to monitor George's emails. ABC

International Data Privacy, continued

Co.'s electronic communications policy may not meet the requirements of the APP, as it does not include all the information required by the APP³³ and does not specifically state that ABC Co. may collect, store, use, and disclose employee emails for purposes of investigations of complaints against employees. ABC Co.'s policy states that it collects and uses these emails for purposes consistent with applicable U.S. laws, but this may not be sufficiently specific to satisfy Australia's transparency requirements.

ABC Co. should be able to rely on the Commonwealth Privacy Amendment's employee records exemption as the authorization for its planned monitoring of George's emails. George is a current employee of the company, and the emails ABC Co. wants to monitor and review are generated and held as a result of George's employment relationship with ABC Co. The company's electronic communications policy will undercut any attempt by George to argue that his emails should not be considered employee records.

If George is working in Sydney, ABC Co. should stop monitoring his emails because its electronic communications policy does not appear to include some of the information required by the Workplace Surveillance Act.³⁴ While it may be detailed by U.S. standards, ABC Co.'s policy does not describe how its monitoring will be carried out. It can be reasonably inferred that ABC Co.'s policy starts when the employee begins work and is ongoing. George could argue, however, that he was not aware of this and did not understand from the notice that this is the policy. ABC Co. will have similar concerns if George works in Canberra during his Australian assignment, as ABC Co.'s policy does not state that an employee can consult with the company about the monitoring.³⁵

Conclusion

While this tale of George's international business trip and the complaints that surfaced once he left the United States is an extreme example of the issues that may arise when an employee is traveling outside the country for business purposes, it highlights the need for

companies to have a "data law checklist" detailing the information they should communicate to the employee, and the acknowledgments they should obtain from the employee, before he boards an international flight. With the appropriate policies and practices, and documentation confirming that the required information was conveyed to the employee during the mandated time frame, employers can ensure that they are in compliance with the applicable international data privacy and protection laws and be confident in their ability to monitor, collect, review, and use the emails of their U.S. employees who are working in countries outside of the United States.

George's ill-fated business trip also demonstrates the importance of educating the company's information technology and human resources professionals on the data protection laws of the countries outside the United States where employees may be working. Without such education and training, and in the absence of detailed and updated policies, information technology and human resources department employees could inadvertently take actions with regard to the emails of employees working in foreign countries that, while legal in the United States, violate the laws of the other countries, thereby potentially creating liability for the company.

Each time the employee's passport is stamped, the applicable data privacy and protection laws change, along with the employer's compliance obligations and its rights to, and restrictions on its entitlement to, monitor, collect, review, and use the emails generated by the traveling employee. Working together, a company's legal, information technology, and human resources departments can put together a data law checklist that ensures that the employee receives the notices required by the countries to which he will be traveling, that the company is able to satisfy its duty to supervise its employees and investigate complaints made against it by monitoring its employee's emails, and that the company is in compliance with the numerous and differing privacy and protection laws in place in countries outside the United States.

International Data Privacy, continued



Lillian Chaves Moon is a partner at Akerman LLP in Orlando, Florida, and is a member of the firm's Labor & Employment and Data Law Practice Groups. She has been practicing employment law for over sixteen years and focuses her practice primarily on representing employers in employment litigation. A

significant portion of her practice is also dedicated to counseling clients on workplace privacy policies and practices, including data breach, HIPAA privacy and security issues, and written information security programs. Furthermore, she provides clients with day-to-day counseling and training to afford the best and most practical solutions that companies can implement in an effort to avoid litigation and to address employment issues as they arise.



Gail Gottehrer is a partner at Akerman LLP in New York, New York, where she is a member of the Labor and Employment Practice Group and the firm's Data Law Practice. Her practice focuses on class action defense, management-side labor and employment litigation, and other complex commercial

matters, including privacy and technology litigation, digital workplace-related actions, and cybersecurity. She is one of the few defense lawyers to have been involved in the trial of a class action to verdict before a jury. She also teaches a course in Law for Knowledge Innovation at Columbia University and is a Fellow of the Center for Innovation at Vermont Law School.

Endnotes

¹ *E.g.*, under Florida's wiretap law, all parties to a communication must consent to have the communication intercepted. The law contains a business extension exception for calls made on a business telephone used in the ordinary course of business, such as recording incoming calls for quality assurance purposes. The interception of a call not made on the business phone or in the ordinary course of business, or an electronic recording (such as an IM) does not fall within that exception, and intercepting such a communication

without the consent of all parties is considered a felony in the third degree. See Fla. Stat. §§ 934.02 and 934.03 (2016).

² Cases regarding whether emails between an employee and his/her attorney generated on the employer's computer system are privileged generally use the following factors to determine whether the employee had a reasonable expectation of privacy in the emails the employee exchanged with his/her attorney: (i) did the company have a policy banning or restricting personal use; (ii) did the company monitor employees' use of email?; (iii) do third parties have a right of access to the computer and email; and (iv) did the company notify the employee or was the employee aware of the use and monitoring policy. See *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 258 (S.D.N.Y. 2005). Courts analyzing these factors have reached different conclusions as to whether the subject emails are privileged, depending on the facts present in each case. For example, in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), the court held that an employee had a reasonable expectation of privacy in email communications with her attorney via her Yahoo account accessed through the employer's computer system where the employer's policy did not clearly specify that "personal, password-protected, web-based email accounts via company equipment [were] covered," and the policy did not provide that the personal emails would be stored on the computer hard drive or within the employer's system. Ownership of the computer system was not the determinative factor. Instead, the court focused on the nature of the emails as privileged communications and the employee's attempt at keeping the communications confidential by using her personal password-protected account. But see *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436 (N.Y. 2007), where the court held that the former employee had waived the attorney-client privilege as to email correspondence with his attorney where he was aware of the employer's policy prohibiting personal use of the employer's computer system and stating that the employer would monitor emails.

³ This article is not meant to be an exhaustive analysis of all applicable laws. There may be other laws in each jurisdiction that employers should consider and factor into their decisions, such as local labor and employment laws, work council or agency guidance, and telecommunications laws. This article addresses only computer systems and devices owned by the employer; it does not discuss the application of these laws to devices used by employees pursuant to an employer's BYOD (bring your own device) policy. Nor does it discuss the legal implications of cross-border data transfers and the shipment of hard drives and other data from countries outside the United States to the United States.

⁴ Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, (Can.), <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-2>.

⁵ *R. v. Cole*, SCC 53, 56, [2012] 3 S.C.R. 34 (Can.).

⁶ *Id.*

⁷ United Kingdom privacy law (as well as the German privacy law discussed *infra*) was developed to meet Council Directive 95/46, which governs the processing of personal data in the European Union and requires each member state to adopt its own law providing the protections set forth in the Directive. In May 2018, the Directive will be replaced by the General Data Protection Regulation (GDPR), which will apply, in pertinent part, to the "processing of personal data of data subjects in the EU by [an employer] not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU." GDPR FAQs,

International Data Privacy, continued

<http://www.eugdpr.org/eugdpr.org.html>. The GDPR will become the law of each member state rather than being a directive to implement a law governing privacy. With Brexit (which will be in effect by the end of March 2019) looming over the UK, legal commentators anticipate the UK will adopt a similar law to the GDPR to give its citizens the same level of protection as that provided in the EU and to obtain approval from the EU to have data transfers readily transmitted between the UK and the EU member state countries. *See id.* The GDPR will require, among other things: (1) informed consent by the employee for monitoring, in a form that is clear and does not contain legalese. The purposes for the monitoring must be limited and specific; (2) the employee must be informed of the types and purposes for which his/her personal data is being processed; (3) the employee has a right of access to the personal data; (4) the employee can request personal data be erased; and (5) the employee can obtain free of charge from the employer a copy of the personal data the employer maintains. *Id.*

8 Regulation of Investigatory Powers Act 2000, c. 23 (Eng.), pt.1, ch. 1, sec., 1(3), <http://www.legislation.gov.uk/ukpga/2000/23/contents>.

9 *Id.* at pt. 1, sec. 3.

10 *Id.* at pt. 1, sec. 1(1).

11 <http://www.legislation.gov.uk/UKPGA/1998/29/contents>.

12 Information Commissioner's Office, Quick Guide to the Employment Practices Code, sec.5 (Eng.), http://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf.

13 *See id.*

14 Additionally, local laws may apply in Germany, as each of its 16 states may also have its own data protection laws. Nolte and Werkmeister, Data Protection in Germany Overview, Thompson Reuters Practical Law, [http://uk.practicallaw.thomsonreuters.com/3-502-4080?__lrTS=20170324004500585&transitionType=Default&contextData=\(sc.Default\)&firstPage=true&bhcp=1](http://uk.practicallaw.thomsonreuters.com/3-502-4080?__lrTS=20170324004500585&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1).

15 Federal Data Protection Act 1998, pt.1, sec. 1(5) (Ger.).

16 Workplace Email Monitoring in Germany, Lexology, <http://www.lexology.com/library/detail.aspx?g=1448cb11-4750-4ce7-a0eb-e2063e043279>.

17 Federal Data Protection Act at pt.1, ch.1, sec. 14(1), https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.html.

18 *Id.* at pt.1, Section 4a(1).

19 *Id.* at pt. 2, ch.1, sec. 32(1).

20 Act on the Protection of Personal Information (Act No. 57 of 2003), ch.1, art. 2(1) (Japan), <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.

21 *Id.* at ch.1, art. 1.

22 Fujiwara and Guesdon, Employment & Labour Law in Japan, Lexology, <http://www.lexology.com/library/detail.aspx?g=c936e099-c578-4105-b2cc-ce96af4d3356>.

23 In the case of a U.S. company with an employee in Australia,

the Privacy Act applies if the company has an "Australian link," which means that the company is either related to an Australian company or carries out business in and the personal information at issue was collected or held by the company in Australia. The Privacy Act of 1998, pt.1, sec. 5(B)(3) (Austl.), <https://www.legislation.gov.au/Details/C2016C00979>.

24 The privacy policy should include: (i) the types of personal information collected; (ii) how the company collects and stores the information; (iii) the purposes for which the company collects, holds, uses, and discloses personal information; (iv) how an individual may access his/her personal information held by the company and seek the correction of the information; (v) whether the company is likely to disclose the personal information to overseas recipients and include the countries where such recipients are located. *Id.* at sch.1, Australian Privacy Principles, pt. 1, sec. 1.4 (a)-(g), <https://www.legislation.gov.au/Details/C2016C00979>.

25 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), sec. 40.6 and 40.7 (Austl.), <http://www.alrc.gov.au/publications/report-108>.

26 The employee record exemption does not apply to job applicants or independent contractors.

27 ALRC Report 108 at sec. 40.12.

28 Workplace Surveillance Act 2005 No. 47, pt. 2, sec. 10(1)-(2) (Austl.). The notice must include information regarding: (i) the type of monitoring (camera, computer, or tracking); (ii) how it will be carried out; (iii) when it will start; (iv) whether it is continuous or intermittent; and (v) whether it will be for a specific period of time or ongoing. *Id.* at sec. 10(4)(a)-(e).

29 *Id.* at sec. 12(b).

30 *Id.* at sec. 19-20.

31 The notice must provide the following information: (i) the type of surveillance device used for the monitoring; (ii) how the monitoring will be conducted; (iii) who will regularly be the subject of the monitoring; (iv) when the monitoring will start; (v) whether the monitoring will be continuous or intermittent; (vi) whether it will be for a specific period of time or ongoing; (vii) the purpose for which the employer may use and disclose surveillance records; and (viii) that the employee can consult with the employer about the monitoring. Workplace Privacy Act 2011, A2011-4, pt.3, div. 3.2, sec. 13, www.legislation.act.gov.au/a/2011-4/current/pdf/2011-4.pdf.

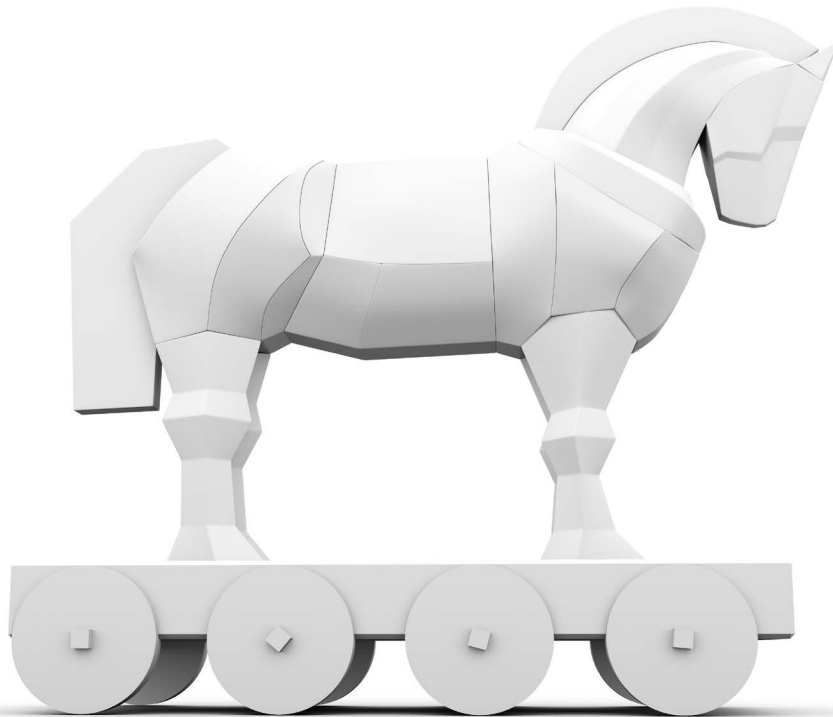
32 For example, the state of Western Australia (which includes Perth) enacted the Western Australia Surveillance Devices Act of 1998 (Austl.), which regulates listening devices, optical surveillance devices, and GPS tracking devices with regard to private conversations and activities. This law, however, does not apply to employer monitoring of emails. Western Australia Surveillance Devices Act 1998, https://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_946_currencies.html.

33 *See* n. 24.

34 *See* n. 28.

35 *See* n. 31.

Protecting Corporate Trade Secrets, from page 19



constitutes a single claim of misappropriation under the DTSA.¹⁶

Damages

DTSA damages include actual losses coupled with any unjust enrichment caused by the misappropriation, or in lieu of damages measured by actual loss, the court may impose liability for a reasonable royalty for a misappropriator's unauthorized disclosure and use of the trade secret.¹⁷ Where the company proves that the misappropriator willfully and maliciously disclosed or removed the trade secret, exemplary damages and attorney's fees may be included to the prevailing party.¹⁸

Defenses

Critically, the "reasonable measures" to protect confidential, proprietary, and trade secret information must be assessed on a case-by-case basis.¹⁹ In other words, public disclosure of the information, lack of any independent economic value to the information,

reverse engineering of the trade secret, independent derivation, or immunization for a whistleblowing employee all provide appropriate defenses to a DTSA claim.²⁰

In the ongoing case of *Worldwide*, the court denied the defendant's motion to dismiss the CFAA and SCA counts of the complaint.²¹ Among other findings, the memorandum opinion referenced the complaint's inclusion of Worldwide's reasonable measures to protect company trade secrets, including a confidentiality agreement, and highlighted the defendant's actions establishing the Google Drive account *in furtherance of his gainful employment* as an agent of Worldwide. Rather than maintaining a personal account sometimes used for business purposes, the "unauthorized access" in Worldwide occurred *after* employment on an account established exclusively for business purposes, so the "haccess" met the threshold elements for the CFAA. Further, the transfer of files and data over the Internet met the requirements of an electronic communication under the SCA.

Protecting Corporate Trade Secrets, continued

Prior to the Enactment of the DTSA

Prior to the enactment of the DTSA and in stark contrast to the above illustration, Central Bank and Trust (Bank) asserted claims against former employees that allegedly transferred confidential, proprietary information, together with trade secrets, to separate Internet drop box locations on alternative servers during their employment. The Bank asserted violations of the CFAA and the SCA, seeking supplemental jurisdiction on various Wyoming state law claims.

The Bank claimed that the former chief financial officer, the assistant cashier, the compliance officer, and the president of the branch each maintained nearly unfettered access to electronic information secured on the plaintiff's servers. The servers were kept under lock and key by the Bank. Only a select number of employees had physical access to the servers. The Bank utilized a number of electronic security protocols, including passwords and different levels of restricted viewing rights for certain employees. The Bank granted each level of access to electronic information based on each employee's particular responsibilities. The employees accessed their information based on their username and password for their computer.

Using Internet-based storage sites, the president of the branch and the chief financial officer copied and diverted information regarding customer details, balance sheets, income statements, overdraft reports, and new loan reports. The Bank considered these documents to be confidential, proprietary, and trade secrets. After transferring voluminous amounts of electronic information to Internet-based drop boxes, even labeling one drop box subfolder with the name of the Bank's competitor state bank, the three employees left to go to work for that competitor approximately a year and a half later.

Even in the face of these allegations, the district court dismissed the entire complaint (including supplemental state law claims) based on a narrow construction and interpretation of the language of the CFAA and the SCA.²² Specifically, the district court reasoned that even if these employees stole company information while still working

for Central Bank and Trust, they did so using the access granted to each of them while gainfully employed by the Bank, so it was not "unauthorized access" in violation of the CFAA or the SCA.

The court construed the language of the CFAA concerning the definitions of "without authorization" and "exceeds authorized access" so as not to include the facts concerning these particular employees because they maintained nearly unfettered access to all information while employed.²³ In concluding, the court emphasized the following "[t]he Computer Fraud and Abuse Act is not an anti-sneaky, disgruntled, and deceitful employee statute. Nor is it an anti-distracted and internet-surfing employee statute. It is an anti-hacking statute. It prevents outside hacking . . ."²⁴ Nonetheless, under the DTSA's "continuing misappropriation" provision, it seems a claim by the Bank may be well taken at this point.

Install Appropriate Countermeasures

In light of the above illustrations, companies should immediately install protective documentation concerning their intellectual property rights, including trade secrets, confidentiality and nondisclosure agreements, noncompete and nonsolicitation agreements, intellectual property rights agreements, etc., along with written notice to all employees from the company regarding whistleblower immunity over any attempt to divert, transfer, download, or otherwise misappropriate confidential, proprietary information, and trade secrets given to a federal, state, or local government official or an attorney.²⁵ By providing this notice, the company may seek inclusion of exemplary damages and attorney's fees under the DTSA.²⁶

Companies must continue to secure their intellectual property and trade secrets using the latest advancements in technology. These include biometric technology requirements for privileged users of data and secure sign-on access to servers for all employees through leading identity assurance providers of multifactor authentication requirements for each end user, especially high-level executives travelling globally.

Protecting Corporate Trade Secrets, continued

These separate requirements must meet the needs of the business through an assessment of the sensitivity of the data being accessed at any given time compared to the business needs to access it.



Joseph T. King practices in the general commercial litigation department of Burr & Forman LLP with a recent focus on representing companies involved in employment litigation. Areas include trade secret litigation, qui tam relator lawsuits, false claim act and anti-kickback statute

investigations, reductions in force, contract negotiations, and other employment law related issues. He resides in Tampa, Florida, and may be reached at (813) 367-5750 or jkking@burr.com.

Endnotes

1 2017 Thales Data Threat Report, Trends in Encryption and Data Security, Global Edition <http://dtr.thalessecurity.com/>. The report surveys more than 1,100 senior Information Technology security executives globally, including 500 companies in the United States, and at least 100 each for the United Kingdom, Germany, Mexico, Brazil, Japan, and Australia.

2 *Id.*

3 *Estes Forwarding Worldwide LLC v. Cuellar*, No. 16-853, 2017 WL 931617 (E.D. VA 9 March 2017).

4 *Id.* at *1.

5 *Id.*

6 *Id.* at *2.

7 *Id.*

8 *Id.*

9 See 18 U.S.C.A. § 1836(b)(1).

10 Peter J. Toren, *The Defend Trade Secrets Act*, 28 No. 7 INTELL. PROP. & TECH. L.J. 3, *9 (2016) (highlighting the extraterritorial

application of the Economic Espionage Act of 1996 that remains in place so that foreign corporations must be particularly sensitive to the reach of the D TSA).

11 See 18 U.S.C.A. § 1836(c).

12 See 18 U.S.C.A. § 1836(b)(2)(A)(i).

13 Bret A. Cohen, Michael T. Renaud, & Nicholas W. Armington, *Explaining The Defend Trade Secrets Act*, BUSINESS LAW TODAY, September 2016, American Bar Association, (noting the definition of a “trade secret” differs from state to state as does the period of limitations on those actions).

14 See 18 U.S.C.A. § 1836(b)(2)(A)(i).

15 See 18 U.S.C.A. § 1836(d).

16 *Id.* See also *Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Group*, No. 16-2499, 2017 WL 1105648, * 8 (E.D. PA 24 March 2017)(finding that Congress clearly expressed its intent to apply the D TSA to continuing misappropriations continuing both prior to and after D TSA’s enactment).

17 See 18 U.S.C.A. § 1836(b)(3)(B).

18 See 18 U.S.C.A. § 1836(b)(3)(C); 18 U.S.C.A. § 1836(b)(3)(D).

19 See *Raben Tire Co., LLC v. McFarland*, No. 16-141, 2017 WL 741569 * 2 (W.D. KY 24 February 2017) (slip copy)(Plaintiff “bears the burden of demonstrating that it took reasonable steps to maintain the secrecy of the protected information.” *Internal citations omitted*).

20 See 18 U.S.C.A. § 1839(6)(B).

21 *Estes Forwarding Worldwide LLC v. Cuellar*, No. 16-853, 2017 WL 931617, *9 (E.D. VA 9 March 2017).

22 *Central Bank and Trust v. Smith*, No. 15-115, 2016 WL 7650644 * 9 (D. WY 31 August 2016).

23 In *Central Bank and Trust v. Smith*, No. 15-115, 2016 WL 7650644 * 4 (D. WY 31 August 2016), the court notes the split between circuits concerning the definitions afforded to the specific statutory construction and interpretation of “without access” and “exceeds authorized access.” Specifically, the 1st, 5th, 7th, and 11th Circuits interpret this language broadly so as to include when someone accesses electronic information with the intent and purpose to misuse that information, even when the person received permission to access the information. The district court in *Central Bank* sided with the 2nd, 4th, and 9th Circuits, dismissing any definition of access that included the subjective area of intent and purpose; instead, adopting a narrow interpretation of the referenced statutory language so as to exclude subjective intent and purpose.

24 *Central Bank and Trust*, 2016 WL 7650644 * 9.

25 See 18 U.S.C.A. § 1833(b).

26 See 18 U.S.C.A. § 1833(b)(3)(C).



Benefits of Section Membership:

- The *International Law Quarterly*
- Writing and Speaking Opportunities
- Discounts for Seminars, Webinars & Downloads
- Section Listserv Notices
- Networking Opportunities
- Great Seminars in Four-Star Hotels at a Group Rate

Invite a colleague to become an ILS member!



Show your pride[®]

The BankAmericard Cash Rewards[™] credit card for The Florida Bar.

1% cash back everywhere, every time

2% cash back at grocery stores **AND NOW AT WHOLESALE CLUBS**

3% cash back on gas

\$100 cash rewards bonus after qualifying purchase(s).[†]

2% and 3% category rewards bonuses apply on up to \$2,500 in combined quarterly spend in those categories.[▼]

To apply visit: newcardonline.com

Use Priority Code VACN5N.

Brought to you by:  Bank of America

For information about the rates, fees, other costs and benefits associated with the use of this Rewards card, or to apply, go to the website listed above or write to P.O. Box 15020, Wilmington, DE 19850.

[▼] The 2% cash back on grocery store and wholesale club purchases and 3% cash back on gas purchases applies to the first \$2,500 in combined purchases in these categories each quarter. After that the base 1% earn rate applies to those purchases.

[†] You will qualify for \$100 bonus cash rewards if you use your new credit card account to make any combination of Purchase transactions totaling at least \$500 (exclusive of any fees, returns and adjustments) that post to your account within 90 days of the account open date. Limit one (1) bonus cash rewards offer per new account. This one-time promotion is limited to new customers opening an account in response to this offer. Other advertised promotional bonus cash rewards offers can vary from this promotion and may not be substituted. Allow 8-12 weeks from qualifying for the bonus cash rewards to post to your rewards balance.

By opening and/or using these products from Bank of America, you'll be providing valuable financial support to The Florida Bar.

This credit card program is issued and administered by Bank of America, N.A. Visa and Visa Signature are registered trademarks of Visa International Service Association, and are used by the issuer pursuant to license from Visa U.S.A. Inc. BankAmericard Cash Rewards is a trademark and Show your pride, Bank of America and the Bank of America logo are registered trademarks of Bank of America Corporation.

©2016 Bank of America Corporation

ARFJCK95

AD-07-16-0242.C

Data Protection in the EU, from page 21

Consistency Throughout the EU—and Even Beyond It

Organizations outside the EU are deemed to be made subject to the jurisdiction of the EU regulators merely by collecting data concerning an EU citizen. While foreign companies might be inclined to challenge that assumption of jurisdiction, it is currently estimated that only having to deal with a single supervisory authority within the EU will produce an estimated savings of €2.3 billion per year (according to EU figures).

What Is “Personal Data”?

“Personal data” is defined in both the Directive and the GDPR as any information relating to a person who can thereby be identified, directly or indirectly.¹ A matter of particular focus will be information that includes

references to identifiers such as a name, an identification number, location data, online identification, or other specifying factors. Of special note here is that online identifiers such as an IP address, “cookies,” and other trackable online data will now in many instances be regarded as personal data. Those instances will typically arise when the potentially identifying data can be linked to a specific individual without extensive effort. For these purposes, no real distinction exists between personal data about individuals arising from activities in their private lives and personal data generated in their performance of work functions.

Data Protection Officers

Data protection officers must be appointed for all public authorities, and where the core activities of



Marchers in Hannover, Germany, protest against the U.S. National Security Agency on 29 June 2013 (Peter Steffen/DPA via the Associated Press).

Data Protection in the EU, continued

the controller or the processor involve “regular and systematic monitoring of data subjects on a large scale” or where the entity conducts large-scale processing of “special categories of personal data” (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and the like).² This rule is expected to apply to, among other types of businesses, larger-scale marketing companies and even research organizations.

An early draft of the GDPR limited mandatory appointment of a data protection officer to organizations with more than 250 employees, but the final version has no such limitation.

The data protection officer’s tasks, as detailed in the regulation, include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws;³
- Monitoring compliance including managing internal data protection activities, training data processing staff, and conducting internal audits;
- Advising with regard to data protection impact assessments when required under Article 33;⁴
- Working and cooperating with the controller’s or processor’s designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data;⁵ and
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

Data protection officers may insist on access to company resources for the purposes of fulfilling their job functions and assisting the company’s personnel in their ongoing training. The officers must have access to the company’s data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line “to the highest management level” of the company. Data protection officers are expressly granted significant independence in their job functions

and may perform other tasks and duties provided they do not create conflicts of interest.⁶

Controllers and Processors

The GDPR does distinguish, however, between the responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide “sufficient guarantees to implement appropriate technical and organisational measures” to meet the regulation’s requirements and to protect data subjects’ rights.⁷

Controllers and processors must “implement appropriate technical and organisational measures” that take into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.”⁸

The regulation provides specific suggestions for what kinds of security actions might be considered “appropriate to the risk,” including:

- The pseudonymization and/or encryption of personal data;⁹
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data;¹⁰
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;¹¹ and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.¹²

Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance.¹³

The controller/ processor relationships must be documented and managed through contracts and protocols that mandate privacy obligations. The upshot is that controllers must assure themselves of processors’ ability to conform to privacy requirements.

Data Protection in the EU, continued

Consent

According to the regulation, consent means “any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.”¹⁴ Although the consent itself need not be explicit, the purposes for which the consent is gained does need to be “collected for specified, explicit and legitimate purposes.”¹⁵ It therefore must be abundantly clear to the data subject what his or her data is going to be used for at the point of data collection.

Consent should be demonstrable and must, not surprisingly, be freely given. Organizations need to be able to show clearly how and when consent was obtained. Consent, once given, can also be withdrawn as to future uses of personal data.

Information Provided at Data Collection

The information that must be made available to a data subject when data is collected is defined to include:

- The identity and the contact details of the controller and the data protection officer;¹⁶
- The purposes of the processing for which the personal data is intended;¹⁷
- The legal basis of the processing;¹⁸
- Where applicable, the legitimate interests pursued by the controller or by a third party;¹⁹
- Where applicable, the recipients or categories of recipients of the personal data;²⁰
- Where applicable, that the controller intends to transfer personal data internationally;²¹
- The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;²²
- The existence of the right to access, rectify, or erase the personal data;²³
- The right to data portability;²⁴
- The right to withdraw consent at any time;²⁵ and
- The right to lodge a complaint to a supervisory authority.²⁶

This list changes when the data has not been obtained directly from the data subject. In that circumstance, the disclosure must make reference to the source from which the personal data originated, and how and why the data was obtained from that source.²⁷ This is likely to cause consternation to marketers using multiple sources of third-party data.

Privacy Management

The GDPR mandates a risk-based approach through which organizational controls must be, in essence, tailored to correspond to the degree of risk associated with the processing activities. Where appropriate, privacy impact assessments must be made, with a focus on protecting data subjects’ rights. Data protection safeguards must be incorporated into products and services from the earliest stage of development. Privacy-friendly techniques such as pseudonymization will be encouraged, to reap the benefits of big data innovation while protecting privacy. There is also an increased emphasis on effective record-keeping for controllers. The critical objectives in this regard are to help demonstrate compliance with the regulation and to improve the capabilities of organizations to manage privacy and data effectively.

Fines and Enforcement

There will be a substantial increase in fines for organizations that do not comply with the new regulation. Regulators will now have authority to issue penalties equal to the greater of €10 million or 2% of the entity’s global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.²⁸

Violations of obligations related to legal justification for processing, data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity’s global gross revenue.

Legitimate Interests and Direct Marketing

The regulation does specifically acknowledge that the

Data Protection in the EU, continued

processing of data for “direct marketing purposes” can be considered as a legitimate interest. Legitimate interest is one of the grounds, like consent, that an organization can invoke in order to process data and satisfy the principle that data has been fairly and lawfully processed. Processing is to be considered lawful if it is “necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”²⁹

Summary and Conclusions

The new EU data protection regime extends the reach of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of data protection regulations throughout the EU, thereby at least theoretically making it easier for non-European companies to comply with these regulations. This comes with undeniable costs, however. The new regulations include a rigorous set of data protection compliance requirements backed by the prospect of severe penalties for noncompliance. Moreover, that new data protection regime’s rigor is not in all respects matched by clarity. The extent to which invocations of “legitimate interest” will effectively be permitted to trump personal data protection is by no means fully understood at this time, and many of the admonitions to data protection officers, controllers, and processors can rightly be critiqued as vague and general, and thus susceptible to selective enforcement (or none at all).

Final implementation of the GDPR will require sweeping changes to business practices for companies that have not to date implemented a comparable level of privacy protection protocols. The European Commission will have to deploy sufficient resources and exhibit sufficient power to enforce implementation and then compliance. None of this is assured. It is all but impossible, however, to envision an attempt at comprehensive, meaningful data protection reform legislation that would not

DID YOU KNOW?

When you register for or purchase a

Florida Bar CLE

you now receive a searchable, downloadable

electronic course book.

This document is sent to you via email before a live course or upon your order of CDs and DVDs. Hard copies of the course book are still available for purchase separately (usually \$60 per book).

The Bar’s CLE programs remain the same quality and low price as always, however, **now the book format is your choice.** For more information, please see course registration forms or visit **www.floridabar.org/CLE**.

Data Protection in the EU, continued

face major enforcement challenges, or that was in all respects clear, specific, and unambiguous. The EU is, at a minimum, to be commended for making an aggressive and thoughtful attempt to combat a rapidly evolving problem.



Philip R. Stein is a partner at Bilzin Sumberg in Miami, Florida. He is an experienced litigator of business disputes, and has extensive experience guiding clients in addressing and mitigating liability related to data security and privacy. Corporate governance is another area of focus for Phil, and he regularly handles

high-stakes cases involving disputes between officers and directors, as well as shareholder litigation. He has extensive experience representing loan originators in mortgage-backed securities and indemnification litigation. In the wake of the financial crisis, he has litigated approximately 100 such cases in jurisdictions around the United States, while securing pre-suit resolutions or settlements in dozens more.

Endnotes

- 1 GENERAL DATA PROTECTION REGULATION [hereinafter GDPR], Article 4, ¶1.
- 2 GDPR, Section 4, Article 37, ¶1(b) and (c).
- 3 GDPR, Article 39, ¶1(a).
- 4 GDPR, Article 39, ¶1(b).
- 5 GDPR, Article 39, ¶1(d) and (e).
- 6 GDPR, Article 38.
- 7 GDPR, (81) at page 50.
- 8 GDPR, Article 24, ¶1; Article 25, ¶1.
- 9 GDPR, Article 32, ¶1(a).
- 10 GDPR, Article 32, ¶1(b).
- 11 GDPR, Article 32, ¶1(c).
- 12 GDPR, Article 32, ¶1(d).
- 13 GDPR, Article 32, ¶3.
- 14 GDPR, Article 4, ¶11.
- 15 GDPR, Article 5, ¶1(b).
- 16 GDPR, Article 13, ¶1(a).
- 17 GDPR, Article 13, ¶1(c).
- 18 GDPR, Article 13, ¶1(c).
- 19 GDPR, Article 13, ¶1(d).
- 20 GDPR, Article 13, ¶1(e).
- 21 GDPR, Article 13, ¶1(f).
- 22 GDPR, Article 13, ¶2(a).
- 23 GDPR, Article 13, ¶2(b).
- 24 GDPR, Article 13, ¶2(b).
- 25 GDPR, Article 13, ¶2(c).
- 26 GDPR, Article 13, ¶2(d).
- 27 GDPR, Article 14.
- 28 GDPR, Article 84.
- 29 GDPR, Article 6, ¶1(f).

Update: Florida Supreme Court to Consider International Litigation and Arbitration Certification

A new International Litigation and Arbitration certification is pending before the Florida Supreme Court. The certification, which was proposed by The Florida Bar's International Law Section, was unanimously approved by the Bar's Board of Governors at its May 2016 meeting. Supreme Court approval is the last step in the approval process. If approved, the International Litigation and Arbitration certification will become the twenty-seventh certification in the Bar's certification program. Although the program has yet to be approved, those who intend to seek certification should begin planning now. Particular attention should be paid this year to meeting the requirements for CLE credit. Specifically, the proposal before the Supreme Court would require applicants to have fifty CLE credits in international litigation and/or arbitration over the five years preceding application.

Maritime Cybersecurity, from page 23

connect the Nation to the global supply chain.”⁸ The benefits of outlining an overarching strategy such as the Coast Guard – Cyber Strategy are clear; however, this document has minimal utility to anyone residing or working outside the Washington, D.C., beltway.

Fortunately, in September 2016, the American Bureau of Shipping (ABS)⁹ finalized its Guide for Cybersecurity Implementation for the Marine and Offshore Industries – CyberSafety Volume 1,¹⁰ which is a certification program for vessel owners and operators. This initial guide from ABS was followed closely by Cybersecurity Implementation for the Marine and Offshore Industries – CyberSafety Volume 2,¹¹ which provided more specific criteria for cybersecurity procedures for the commercial maritime industry. Additionally, several other classification societies, including Lloyd’s Register and DNV GL,¹² have also instituted maritime cybersecurity certification programs for vessels and the maritime

industry. The classification societies’ newly implemented cybersecurity guidelines reflect the maritime industry’s awareness of the importance of protecting the technology and information systems that currently drive global maritime commerce. A review of both ABS’s and Lloyd’s Register’s cybersecurity guidelines reflects that one size does not fit all, as the key component of improving maritime cybersecurity is the identification of the vulnerabilities in the maritime electronic information systems that are in use and on board a specific vessel or fleet of vessels. Despite the challenges of addressing cybersecurity in the maritime transportation system, the international classification societies are rightly taking the lead in this undertaking, one vessel at a time.

The Voyage Data Recorder and Automatic Information Systems

Two key pieces of technology on the bridge of nearly



Maritime Cybersecurity, continued

all commercial vessels today merit close consideration when analyzing cybersecurity vulnerabilities in the maritime realm: (1) the voyage data recorder (VDR); and (2) the automatic information system (AIS) transponder. In 2000, the IMO adopted a requirement (as part of a revision to SOLAS chapter V) that all passenger vessels and cargo vessels over 300 gross tons engaged in international trade carry automatic identification systems. The AIS transponder allows for the transmission of the following information to other ships and to the coastal authorities and port authorities: (1) vessel name; (2) vessel type; (3) vessel position; (4) course; and (5) speed. The IMO has published guidelines that detail the interface between the AIS and the data inputs from the vessel's navigation equipment.¹³ Indeed, the IMO guidelines specifically state, "The sensor information transmitted by AIS should be the same information being used for navigation of the ship."¹⁴ AIS is a technology that clearly improves the efficiency and safety of maritime transportation by minimizing the risk of collisions and allowing customers to track the vessels that are carrying their shipments and goods. One of the initial cybersecurity issues with AIS is that real-time AIS data is now freely available on the World Wide Web. Websites such as Marinetransport.com publish real-time AIS data for nearly every commercial vessel equipped with an AIS transponder. Another issue related to AIS is in relation to the SOLAS mandate that the AIS should always be switched "on." What happens when a vessel switches the AIS "off"? With its AIS switched "off," a vessel disappears from the AIS tracking systems of the coastal states and port authorities. A recent investigation conducted by maritime analytics firm Windward and the *International Business Times* suggests that in January and February of 2017, more than 2,800 vessels had switched off their AIS prior to entering European waters.¹⁵ The cybersecurity risks are clear in that the easy access to AIS data allows for the malicious targeting of strategically important vessels and, conversely, by shutting off the AIS, a rogue vessel can mask its location to aid in smuggling or possibly terrorist attacks.

A voyage data recorder (VDR) is similar to a "black box" in a commercial airliner and is required to be

carried on passenger ships and cargo ships of 3,000 gross tons or more in order to assist in marine accident investigations. The mandatory regulations related to VDRs are contained in chapter V of SOLAS and include performance standards for VDRs, which detail the data to be recorded. A VDR continuously maintains sequential records of data items relating to status and output of the ship's equipment, navigation, and command and control of the ship. The data inputs to the VDR include: (1) Global Positioning System (GPS) data; (2) electronic charting data; (3) speed log data; (4) gyrocompass heading; (5) clinometer; (6) AIS data; (7) radar data; (8) bridge audio; (9) VHF radio communications; (10) electronic log books; (11) bow thruster orders; (12) rudder orders; and (13) engine orders. One of the main advantages for those who investigate marine incidents is the VDR's capability of capturing the actual conversations between crew members on the bridge and being able to compare the conversations with the hard data related to the vessel's location and navigation collected by the VDR.

Indeed, determining the causes of a marine incident will often hinge on understanding how the watch officer or vessel's master understood the navigation data and communicated to crew members regarding the situation. For example, the successful recovery of the VDR from the M/V El Faro, the U.S.-flagged cargo ship that sank during Hurricane Joaquin in October 2015, revealed important information regarding the conversations on the bridge of the vessel in the twenty-six hours prior to its loss.¹⁶ Apart from providing marine investigators with vital information regarding an accident, maritime lawyers often seek to use data, information, and communications recovered from a VDR in litigation. *See, e.g., In re Foss Mar. Co.*, 2015 U.S. Dist. LEXIS 87540 (W.D. Ky. July 6, 2015)(discussing the admissibility of transcripts derived from the audio recordings from a vessel's voyage data recorder); *Ms Tabea Schiffahrtsgesellschaft MbH v. Bd. of Comm'rs of the Port of New Orleans*, 2010 U.S. Dist. LEXIS 103171 (E.D. La. Sep. 29, 2010)(VDR data utilized by expert witness to create computer reconstruction of a vessel grounding and allision). Additionally, the location and custody of the VDR is also sometimes a

Maritime Cybersecurity, continued



fake civilian GPS signals to slowly block and replace the authentic GPS signals being sent to a large vessel until the researchers were able to obtain control of the ship's navigation system to make course and speed adjustments.²⁰ The newer versions of the commercially available VDRs allow for the connection of data inputs within a local area network to be connected to the VDR through ethernet. With every key piece of electronic equipment tied into and providing inputs to the VDR, the need to ensure the integrity of the data inputs to the VDR is clear.

Just Over the Horizon

We all read daily that companies such as Uber and Google are working on and testing autonomous cars and trucks. It should come as no surprise that the maritime industry is also experimenting with autonomous vessels²¹ and is perhaps only a couple of years away from the first commercial maritime delivery of goods

key issue in litigation. In *Abeid-Saba v. Carnival Corp.*,¹⁷ Florida's Third District Court of Appeal upheld an order granting the dismissal, based on forum non conveniens, of claims related to the tragic grounding in 2012 of the cruise ship M/V Costa Concordia off the coast of Italy. In upholding the dismissal, the Third District Court of Appeal specifically referenced the fact that the VDR for the M/V Costa Concordia was in the custody of the Italian authorities to support the trial court's holding that litigating in Florida would result in a material and manifest injustice due to the cost and limited access to relevant evidence.¹⁸

It is clear that the data recorded¹⁹ in a vessel's VDR is vital to any accident investigation; however, it is the very interconnectedness of the navigation data inputs to the VDR and the AIS that pose a significant cybersecurity risk to the maritime industry. Nearly every modern vessel has an electronic auto-pilot that is connected to the vessel's GPS transceiver. The risks inherent to the interface of all of the vital bridge navigation equipment were illustrated in 2013 when a University of Texas researcher utilized

and raw materials with an autonomous or remotely piloted container vessel, bulk cargo vessel, or tanker. For example, Rolls Royce is partnering with DNV GL and Inmarsat, among others, to fund the Advanced Autonomous Waterborne Applications Initiative (AAWA).²² The AAWA partnership is working on the specifications and designs for autonomous commercial vessels and for remotely operated commercial vessels. The initial proposals for only the navigational inputs for autonomous and remotely piloted commercial vessels include the connectivity of the following electronic instruments: (1) cameras; (2) short range radar; (3) long range radar; (4) GPS; (5) electronic navigational charts; and (6) a microprocessor to sensor and analyze data inputs.²³ Indeed, separate electronic input systems for propulsion control systems, engineering auxiliary systems, steering systems, and collision avoidance systems would also need to be perfected prior to any operational testing of autonomous or remotely piloted commercial vessels. It is not hard to imagine a terrorist attempting to hack into a remotely piloted commercial vessel in order to cause a catastrophic environmental

Maritime Cybersecurity, continued

event or to scuttle a vessel to disrupt port cargo operations. It is clear that the cybersecurity risks in the maritime realm will only be compounded as the technology associated with autonomous commercial vessels is brought to market and implemented.

Technology on board commercial vessels is rapidly changing and helping to improve efficiencies in global commerce. These efficiency improvements have been widespread and have touched nearly every nation on the globe. As the commercial maritime transportation industry continues to leverage technology, it is imperative to ensure that proper safeguards and procedures are in place to identify cybersecurity issues and vulnerabilities before a malicious cyberattack occurs in the maritime realm. Industry, flag states, classification societies, and regulatory agencies need to work closely in order to identify the vulnerabilities to the increasingly tech-driven maritime transportation network.



Ryon L. Little is an attorney with *De Leo & Kuylenstierna PA* in Miami, Florida, and focuses his practice on admiralty and maritime law, including all facets of litigation involving commercial vessels and pleasure craft related to marine environmental claims, collisions,

groundings, defense of maritime death and injury claims, crew claims, marine contracts, protection and indemnity matters, regulatory issues, internal investigations of marine casualties, and salvage claims. During law school, he was mobilized for active duty on four occasions as a member of the U.S. Coast Guard Reserve. He has over four years of sea duty as a deck watch officer and boarding officer and served as the executive officer of a Coast Guard cutter.

Endnotes

1 Schmitt, Michael N., *The Law of Cyber Targeting*, NAVAL WAR COLLEGE REVIEW, Vol. 68, No. 2, 11, 19 (Spring 2015).

2 George, Rose, *Ninety Percent of Everything: Inside Shipping, the Invisible Industry That Puts Clothes on Your Back, Gas in Your Car, and Food on Your Plate*, (1st Ed. 2013).

3 “Just-in-time” inventory planning is a strategy employed to increase efficiency and decrease waste by receiving goods only as they are needed in an effort to reduce inventory costs.

4 The IMO is a specialized agency of the United Nations that acts

as a standard-setting authority for issues related to safety, security, and environmental impacts of the maritime industry.

5 46 U.S.C.S. § 70101 et seq. (Public Law 107-295, 25 Nov. 2002).

6 The document can be found at <http://www.uscg.mil/SENIORLEADERSHIP/DOCS/cyber.pdf>.

7 United States Coast Guard, *United States Coast Guard - Cyber Strategy* (June 2015); found at <http://www.uscg.mil/SENIORLEADERSHIP/DOCS/cyber.pdf>.

8 See footnote 7 at page 31.

9 The American Bureau of Shipping, commonly referred to as ABS, is a classification society that develops and verifies standards for the design, construction, and operational maintenance of marine-related facilities and vessels. A classification society also validates that construction of vessels is done according to standards and will carry out regular surveys to ensure compliance with the applicable standards and flag state regulations.

10 The document can be found at http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf.

11 The document can be found at http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety_V2_Cybersecurity_Guide_e.pdf.

12 DNV GL was formed when Det Norske Veritas (Norway) and Germanischer Lloyd (Germany) combined in 2013 to create the world’s largest classification society.

13 Guidelines for the Installation of Shipborne Automatic Identification System (AIS), International Maritime Organization, SN/Circ. 227, 6 January 2003.

14 See footnote 13, section 4.

15 Haddad, Tareq, “Ghost Ships” en route to UK Raise Terror Fears by “Going Dark”, (10 March 2017) at <http://www.ibtimes.co.uk/ghost-ships-en-route-uk-raise-terror-fears-by-going-dark-1610760> (last visited 29 March 2017).

16 26 Hours of Information Recovered from El Faro Voyage Data Recorder, National Transportation Safety Board press release, <https://www.nts.gov/news/press-releases/Pages/PR20160824.aspx> (last visited 29 March 2017).

17 184 So. 3d 593 (Fla. 3d D.C.A. 2016).

18 See footnote 17.

19 It is important to note that VDRs routinely overwrite the stored data inputs. Older versions of VDRs can overwrite data every 12 hours, and VDRs installed after 1 July 2014 need to store data for 48 hours. Either way, a marine investigator or maritime lawyer needs to be aware of these limitations on data storage capabilities of the VDR at issue.

20 UT News, *Spoofing a Superyacht at Sea*, (30 July 2013), <https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea> (last visited 29 March 2017).

21 The International Convention for the Safety of Life at Sea (SOLAS), 1974, mandates that each flag state be responsible for issuing safe manning certificates for commercial vessels under its flag. Similarly, the Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs) requires, among other things, that each vessel have a lookout. This poses an interesting maritime law issue wherein autonomous and remotely piloted vessels would have no humans on board. Thus, new rules for the certification of autonomous and remotely piloted commercial vessels would need to be developed in order to ensure compliance with the international conventions.

22 The AAWA white paper can be found at <http://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawawhitepaper-210616.pdf>.

23 See footnote 22, AAWA white paper at page 19.

International Legal Assistance, from page 25

cases, [an] obstacle is the more limited capacity of some foreign law enforcement agencies to conduct sophisticated forensic searches of subject computers.”²⁰ Commentators believe this perceived disadvantage of MLATs often leads the DOJ to seek a search warrant instead, as evidenced by *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) (hereinafter *Microsoft*).²¹ *Microsoft*, however, reinforces the continued importance of MLATs in criminal matters where data is located in a foreign jurisdiction. As discussed below, the Second Circuit has been unreceptive to arguments that the MLAT process is “cumbersome.”

In December 2013, federal agents issued a search warrant against Microsoft pursuant to § 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* (SCA), seeking information associated with a Microsoft user’s web-based email account. The emails that the government sought, however, were located in a data-storage center in Dublin, Ireland. Microsoft argued that collection of the data—either directly by the U.S. government or by Microsoft’s U.S.-based employees—would constitute an extraterritorial seizure. Microsoft argued that the United States would have to proceed under its MLAT with Ireland to properly seize the data in Ireland, and that its failure to do so may violate international law.²² Ireland took the same position.²³ Microsoft also argued that the SCA’s use of the term *warrant* meant to incorporate the traditional territorial limitations of search warrants, noting that under Fed. R. Crim. P. 41, federal agents can seize items at locations in the United States and in U.S.-controlled areas, but their authority generally does not extend further.²⁴ Accordingly, for purposes of assessing its extraterritorial effect, Microsoft urged the court not to treat an SCA search warrant any differently than a Rule 41 search warrant.

The government focused on the SCA’s text and structure²⁵ to suggest that an SCA warrant had features of both a traditional search warrant and a subpoena “because a subpoena—generally unlike a warrant—is

executed by a service provider rather than a government law enforcement agent and because it does not require the presence of an agent during its execution.”²⁶ Analogizing to the rules governing subpoenas, the government argued that it was the location of the entity (Microsoft) with control over the data that matters and, therefore, asking Microsoft’s U.S.-based employees to access the Ireland-based data did not present extraterritoriality issues.²⁷

The district court rejected Microsoft’s extraterritoriality argument, concluding that it was the location of the provider (i.e., Microsoft) and not the location of the data that controlled. Relatedly, the district court treated the location where the government would review the content (the United States), not the location of storage (Ireland), as the relevant point of seizure.²⁸ The district court reasoned that Microsoft employees located in the United States could access and retrieve the Ireland-based data and, thus, the SCA search warrant was proper.²⁹

On 14 July 2016, the Second Circuit reversed the district court and held that the SCA search warrant was invalid. The court rejected the government’s argument that “similar to a subpoena, an SCA warrant requires the recipient to deliver records [and data] to the government no matter where those documents are located, so long as they are subject to the recipient’s custody or control.” *Id.* at 201. The court stated that “[n]either explicitly nor implicitly does the [SCA’s statutory text] envision the application of its warrant provisions overseas.”³⁰ The court considered the SCA’s use of the term *warrant* significant, and its use led the court to conclude that “Congress intended to invoke the term ‘warrant’ with all of its traditional, domestic connotations.”³¹ Since its passage in 1986, Congress has amended § 2703 to relax some of the Rule 41 requirements as they relate to SCA warrants, but the court determined that “none of the amendments contradicts the term’s traditional domestic limits [and the amendments were] fully consistent with the historical role of warrants as legal instruments that pertain to discrete objects located within the United States, and that are designed to protect U.S. citizens’ privacy interests.”³²

The Second Circuit was unsympathetic to the district

International Legal Assistance, continued

court's observation that "the current [MLAT] process for obtaining foreign-stored data is cumbersome" and viewed its holding as consistent with "the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations."³³ The court admitted that it could not be certain "of the obligations that the laws of [Ireland or the EU] place on a service provider storing digital data . . . within its territory," but declined to disregard those obligations "on the theory that [Ireland's] interests are unaffected [by] an order requiring a service provider to 'collect' and 'import' into the United States data [from Ireland-based servers] . . . simply because that service provider [operated] within the United States."³⁴ In a victory for the MLAT process, the court viewed enforcement of the warrant as an unlawful extraterritorial application of the SCA "insofar as it direct[ed] Microsoft to seize the contents of its customer's communications stored in Ireland."³⁵

In the Second Circuit's view, if the U.S. government wanted the communications stored in Ireland, it would have to obtain them through the MLAT process.

Do the Recent Rule 41 Amendments Foretell Similar Changes to 18 U.S.C. § 3512?

While *Microsoft* reiterated the primacy of MLATs over search warrants under certain circumstances, recent changes to Fed. R. Crim. P. 41 ("Search and Seizure") aimed at streamlining domestic searches of electronic storage media call into question whether 18 U.S.C. § 3512's long-

standing limitation on the handling of MLAT requests for Rule 41 search warrants should continue. In 2016, Congress considered proposed amendments to Rule 41, which took effect on 1 December 2016. The DOJ perceived the prior version of Rule 41 as falling short in "two increasingly common situations": (1) where the proposed search warrant was able to describe sufficiently the computer to be searched, but the district within which that computer was located was unknown for one reason or another; and (2) where the investigation required law enforcement to coordinate



searches of numerous computers in different districts.³⁶

Rule 41's new provisions expand its reach in judicial districts beyond the jurisdiction where the search warrant application is reviewed.³⁷ New subsection 41(b)(6)³⁸ authorizes a court to issue a warrant to search electronic storage media and to seize ESI inside or outside of the judge's district: (1) when "the district where the media or information is located has been concealed through technological means"; or (2) in an investigation into a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5), when the media to be

International Legal Assistance, continued

searched includes affected computers located “in five or more” districts—an often vexing issue in investigations involving a dispersed hacking consortium taking part in malware or ransomware attacks.³⁹

Given these recent changes to Rule 41 aimed at streamlining the search warrant process in certain domestic cybercrime contexts, it will be interesting to see whether Congress will amend 18 U.S.C. § 3512 to include similar provisions when judges handle MLAT requests seeking Rule 41 search warrants. Presently, 18 U.S.C. § 3512(d) expressly excludes Rule 41 search warrants from 18 U.S.C. § 3512’s streamlining provision that allows district court judges handling MLAT requests to oversee and approve subpoenas and other orders with effect in districts other than their own.⁴⁰ Thus, under Section 3512’s current language, a foreign sovereign’s MLAT request for a Rule 41 search warrant requires the prosecutor handling the request to apply for the search warrant in the district where “the place or person to be searched” is located, thereby maintaining the logistical impediments that motivated the recent Rule 41 amendment.⁴¹ The most efficient amendment to Section 3512 would be a simple deletion of Section 3512(d)’s limitation, which would allow Section 3512(a)(2)’s reference to Rule 41 to be coextensive with Rule 41’s new parameters. Alternatively, Congress could expressly amend Section 3512 to allow the prosecutor handling the MLAT request(s) to seek an out-of-district Rule 41 search warrant subject to limitations similar to those in Rule 41(b)(6). After all, one could argue that the same concerns that led to Rule 41(b)(6)’s creation might also arise under Section 3512 when a foreign sovereign seeks a search warrant as part of its own cybercrime investigation. Either of these amendments would arguably: (1) create consonance between Rule 41’s updated language and Section 3512; (2) promote comity interests;⁴² and (3) further the statutory purposes of Section 3512 as well as the public policy underlying MLATs.⁴³

Conclusion

As this article illustrates, foreign legal assistance in the

criminal sphere can take multiple forms depending on the facts and the legal relationship between the United States and the foreign government in question. In the cybercrime context, a proper understanding of the legal framework for seeking such foreign assistance should not escape any civil or criminal practitioner advising the cybercrime victim or discovery targets of a cybercrime investigation. Estimates indicate that cybercrime “will become a \$2.1 trillion problem by 2019,” and its steady rise has been described as “nothing short of epic.”⁴⁴ Given the growing transnational dimension of cybercrime, one can anticipate that the United States and foreign governments will see a steady increase in MLAT requests aimed at securing cybercrime-related evidence.



Armando Rosquete is an attorney at Boies Schiller Flexner LLP, a former assistant United States attorney (2006-2012), a former law clerk for Justice Raoul G. Cantero III on the Florida Supreme Court, and a graduate of Harvard Law School (2003). His practice focuses on complex commercial litigation and white-collar criminal defense.

Endnotes

1 See Hon. Virginia M. Kendall & T. Markus Funk, *The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence*, LITIGATION, Winter 2014, at 59 (“We live in a world that appears smaller each day due to the ease of instantaneous electronic communication. Not surprisingly, the criminal’s ability to cross international borders to commit crimes, store evidence, and employ codefendants in foreign countries is correspondingly on the rise . . .”).

2 See § 21:91, Letters Rogatory, 3 Bus. & Com. Litig. Fed. Cts. § 21:91 (4th ed.); *U.S. Attorney’s Criminal Resource Manual*, § 275 (“Letters Rogatory”), available at <https://www.justice.gov/usam/criminal-resource-manual>.

3 See *U.S. Attorney’s Criminal Resource Manual*, *supra* note 2, § 275 (“Letters Rogatory”).

4 Recognizing the delays inherent in securing evidence from abroad, Congress has enacted provisions for suspending the statute of limitations and the requirements of the Speedy Trial Act during the pendency of a formal request for international judicial assistance; however, the suspensive effect is not automatic. See 18 U.S.C. §§ 3161(h)(9), 3292 (involving Speedy Trial Act and statute of limitations respectively); see also *U.S. Attorney’s Criminal Resource Manual*, *supra* note 2, § 272 (“Statute of Limitations and Speedy Trial Act”).

5 See *U.S. Attorney’s Criminal Resource Manual*, *supra* note 2, § 276 (“Treaty Requests”).

International Legal Assistance, continued

6 Yonatan L. Moskowitz, *MLATs and the Trusted Nation Club: The Proper Cost of Membership*, 41 *YALE J. INTL. L.* Online 1, 3 (2016).

7 See *U.S. Attorney's Criminal Resource Manual*, *supra* note 2, § 266 ("International Legal Assistance").

8 See Kendall & Funk, *supra* note 1, at 61; see also Moskowitz, *supra* note 6, at 2 n.5 ("The United States had signed MLATs with sixty-four countries, fifty-eight MLATs were in force as of 2013.").

9 See Kendall & Funk, *supra* note 1, at 59.

10 While MLATs do not allow an individual to seek evidence under their provisions, there is somewhat of an open question as to whether, under certain circumstances, a private party can seek redress through an MLAT request facilitated by the party's home country. See, e.g., *Weber v. Finker*, 554 F.3d 1379, 1384 (11th Cir. 2009) (discussing this issue).

11 See Kendall & Funk, *supra* note 1, at 59, 61 (stating that defense counsel may well argue that a vital piece of exculpatory evidence is located overseas and that the MLAT process is the only realistic way of obtaining it and that this argument, in the right case, may have some basic appeal).

12 The statute went into effect 19 October 2009.

13 155 Cong. Rec. S6809-10 (daily ed. 18 June 2009) (statement of Sen. Whitehouse).

14 *In re Request from United Kingdom Pursuant to Treaty Between Gov't of U.S. & Gov't of United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price*, 685 F.3d 1, 11 (1st Cir. 2012) ("Among other differences, § 3512 provides for a more streamlined process than under § 1782 for executing requests from foreign governments related to the prosecution of criminal offenses.").

15 *Weber*, 554 F.3d at 1384 (involving a Swiss citizen who was facing a criminal investigation in his home country and used 28 U.S.C. § 1782 to obtain evidence and noting that "Congress clearly intended for § 1782 to facilitate discovery . . . for use in foreign criminal actions").

16 See *In re Commissioner's Subpoenas*, 325 F.3d 1287, 1290 (11th Cir. 2003), *abrogated in part by Intel Corp. v. Advanced Micro Devices, Inc.*, 542 U.S. 241 (2004) ("Despite the apparent versatility of 28 U.S.C. § 1782, law enforcement authorities found the statute to be an unattractive option in practice because it provided wide discretion in the district court to refuse the request and did not obligate other nations to return the favor that it grants.").

17 *Dolours Price*, 685 F.3d at 11 n.13 (highlighting difference between 28 U.S.C. § 1782 and 18 U.S.C. § 3512).

18 See 18 U.S.C. § 3512(c)(2); Kendall & Funk, *supra* note 1, at 59 ("Section 3512 . . . permits a single prosecutor to pursue requests in multiple judicial districts, eliminating the need for judges in different



districts to appoint commissioners and otherwise duplicate their efforts.").

19 *Dolours Price*, 685 F.3d at 11 n.13 (citing 18 U.S.C. § 3512(f) and noting same).

20 See Kendall & Funk, *supra* note 1, at at 61.

21 See Jennifer Daskal, *The Un-Territoriality of Data*, 125 *YALE L.J.* 326, 393–94 (2015) ("But the MLAT system has historically been slow and clumsy, which is precisely why the government [in the *Microsoft* case was] seeking to get the data directly from the ISPs. The United States, for example, takes an average of ten months to respond to law enforcement requests made pursuant to the MLAT process; other nations take longer.").

22 See Daskal, *supra* note 21, at 57-60, *Microsoft*, No. 14-2985-CV (2d Cir. 8 Dec. 2014); Brief for Ireland as Amicus Curiae Supporting Appellant at 4, 7, *Microsoft*, No. 14-2985-CV (2d Cir., 23 Dec. 2014).

23 *Id.*

24 See *Microsoft*, 829 F.3d at 209 ("Microsoft offers a different conception of the reach of an SCA warrant. It understands such a warrant as more closely resembling a traditional warrant than a subpoena. In its view, a warrant issued under the Act cannot be given effect as to materials stored beyond United States borders, regardless of what may be retrieved electronically from the United States and where the data would be reviewed.").

International Legal Assistance, continued

25 See, e.g., 18 U.S.C. § 2703(g) (“Presence of Officer Not Required”) (“[T]he presence of an officer shall not be required for service or execution of a search warrant issued in according with this chapter . . .”).

26 See *Microsoft*, 829 F.3d at 209 (“Adopting the government’s view, the magistrate judge denied Microsoft’s motion to quash, resting on the legal conclusion that an SCA warrant is more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it is stored at premises ‘owned, maintained, controlled, or operated by Microsoft Corporation.’”).

27 *Id.*

28 *Id.* at 204.

29 See *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (containing factual and procedural history of the case).

30 *Microsoft*, 829 F.3d at 201.

31 *Id.* at 213.

32 *Id.*

33 *Id.* at 221.

34 *Id.*

35 *Id.*

36 See “Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure” (Sept. 2015) at 25-26 (hereinafter “Judicial Conference Report”), available at http://www.uscourts.gov/sites/default/files/st09-2015_0.pdf (summarizing proposed changes to Fed. R. Crim. P. 41); see also Leslie R. Caldwell, “Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches,” (20 June 2016), available at <https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches> (discussing the investigations impacted by the changes to Fed. R. Crim. P. 41).

37 See Judicial Conference Report at 25, n. 5 (noting that prior version of Rule 41 only authorized search warrants for property located outside the judge’s district “in only four situations: (1) for property in the district that might be removed before execution of the warrant; (2) for tracking devices installed in the district, which may be monitored outside the district; (3) for investigations of domestic or international terrorism; and (4) for property located in a U.S. territory or a U.S. diplomatic or consular mission.”).

38 Rule 41(b)(6) provides as follows:

(6) a magistrate judge with authority in any district where activities

related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Fed. R. Crim. P. 41(b)(6). 18 U.S.C. § 1030(a)(5) is part of the criminal statute concerning “fraud and related activity in connection with computers.”

39 See Judicial Conference Report, *supra* note 34, at 25.

40 See 18 U.S.C. § 3512(d) (“Search Warrant Limitation”) (“An application for execution of a request for a search warrant from a foreign authority under this section, other than an application for a warrant issued as provided under section 2703 of this title, shall be filed in the district in which the place or person to be searched is located.”).


41 *Id.* (“An application for execution of a request for a search warrant from a foreign authority under this section . . . shall be filed in the district in which the place or person to be searched is located.”).

42 See *Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern Dist. of Iowa*, 482 U.S. 522, 544, n. 27 (1987) (“Comity refers to the spirit of cooperation in which a domestic tribunal approaches the resolution of cases touching the laws and interests of other sovereign states.”).

43 See, e.g., *United States v. Trustees of Boston Coll.*, 831 F. Supp. 2d 435, 450 (D. Mass. 2011), *aff’d in part, rev’d in part*, 718 F.3d 13 (1st Cir. 2013) (“MLAT requests are intended to improve law enforcement cooperation between nations . . . One important aspect of MLAT requests is the need for speed in processing requests by other nations, as ‘[s]etting a high standard of responsiveness will allow the United States to urge that foreign authorities respond to our requests for evidence with comparable speed.’ 155 Cong. Rec. S6810 (daily ed. 18 June 2009) (statement of Sen. Whitehouse) (discussing 18 U.S.C. § 3512).”).

44 Limor Kessem, *2016 Cybercrime Reloaded: Our Predictions for the Year Ahead*, SECURITY INTELLIGENCE (15 Jan. 2016), available at <https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/>.

ETHICS QUESTIONS?



Call The Florida Bar’s

ETHICS HOTLINE

1/800/235-8619

Internet Regulation and Data Protection, from page 27

over how this new medium would be regulated. The prospect of online markets and unlimited information sharing quickly drew the attention of companies and governments that sought to exercise some control over cyberspace.¹⁷

In response to this first attempt at regulation, John Perry Barlow famously proclaimed the independence of cyberspace in 1996, claiming that this new environment should not be violated by state entities.¹⁸ Clearly, there was much idealism concerning the perfect equality and interaction that the network provided, where people were not affected by their physical or social aspects. Also, since the early “netizens” (so-called citizens of the Internet) were mostly techies or people who had higher computer skills, the ability to interact with this crude environment led to the illusion that the users could tailor their systems, guaranteeing free expression and liberties to all.¹⁹

The cyberspace rapidly expanded in functionalities and appliances. Newer browser interfaces, new layers, faster connections, and other features led the cyberspace to extrapolate its merely communicational purposes, and its horizon of possibilities soon demanded state intervention.²⁰ The great challenge, it seemed, was that the Internet was everywhere—today taken to the extreme of the Internet of Things—so that no particular state could properly regulate it. Regulation, however, was essential to guarantee all that the Internet could offer. In order to allow electronic commerce, the state would need to guarantee property and contract rights in the same way it did in the physical world. To hasten bureaucratic governmental processes, the state would need to guarantee that the documents circulating on the Internet could be verified in some way.

Soon, the threats also appeared. This network that brought numerous liberties also provided means of new violations. With database violations, copyright infringement, and server attacks, the companies using the Internet *needed* institutional protection in order to operate. The absence of the state would, in essence, jeopardize everything the Internet had to offer.

The bottom-up regulatory model of the cyberlibertarians soon showed its weaknesses. The global anarchy it proposed clearly would not suffice to meet the needs of interacting states, populations, and markets. In the late 1990’s, this was more than clear, and in 1996, Lawrence Lessig had already challenged Barlow’s view of cyberspace by proposing a very present state in the Internet, through his book *Code 1.0*.

Who Are the Cyberpaternalists and What Do They Believe?

After cyberlibertarians had declared cyberspace a territory of liberties, not under state control in terms of borders and sovereignty, including Barlow who proclaimed its independence,²¹ cyberpaternalists presented questions that remain unanswered.

One of those issues concerns intangible borders and regulatory procedures. For example, how can China, North Korea, and Saudi Arabia control, filter, and blacklist websites and prohibit certain software in their territory?²² Or, for instance, how is it possible for Uber to be prohibited in some clearly defined physical boundaries?²³ Also, in an attempt to propose an opposing point of view, if the cyberlibertarians are correct, how should states deal with anonymity and crimes in the deep web—named *Dot Onion/Tor*,²⁴ child pornography,²⁵ cyberbullying,²⁶ porn revenge,²⁷ cybercrimes,²⁸ data privacy violations,²⁹ disruptive services,³⁰ thefts/extortion³¹ on bank accounts, and money laundering?³² As Cass Sunstein³³ stated, it is unimaginable for cyberspace to be a democratic place without some kind of state intervention, since we do not know who represents and speaks on behalf of society.³⁴ Representation and accountability are two of the most difficult political elements of democracy, lost amidst the crowd in cyberspace.³⁵ Deliberation and decision processes in cyberspace, for example, present a new challenge in an environment where we cannot ensure that democratic values will be developed.³⁶

Cyberlibertarianism is an approach that ignores the fact that cyberspace is different from physical life, above all in its capacity to connect people who have the same

Internet Regulation and Data Protection, continued



interests and to allow people to isolate themselves based on their differences. In fact, it is flagrant that governments send legal messages by regulating certain activities in order to influence the architecture of the network. France³⁷ and Australia,³⁸ for example, have just passed and upheld laws that use filtering and blacklisting controls for surveillance and for the protection of copyrights. Airbnb and Uber are changing their policies on home sharing and transport, respectively, after England and France adopted new legislation on taxed services.³⁹

The first theorist to criticize the flaws of cyberlibertarianism was Joel Reidenberg,⁴⁰ despite his agreement with Post and Johnson about imaginary boundaries and the disintegration process of territorial references. As the founder of cyberpaternalistic theory, Reidenberg established a comparison of a new rule of

law in cyberspace with the *lex mercatoria*, which he called *lex informatica*. For him, cyberspace was not immune to regulatory interventions; since, according to Andrew Murray,⁴¹ he identified two new regulatory borders arising from new rule-making processes involving states, the private sector, technical interests, and citizens. These components had special roles for Reidenberg and were based on contractual agreements among internet service providers (ISPs) and network architecture, becoming the new borders made and controlled by society.⁴² In sum, *lex informatica* would be the stakeholders' new model of political governance in cyberspace,⁴³ in which the regulatory process must be understood in another context, especially because legal control would be just one aspect of regulatory practice as a whole.⁴⁴

Reidenberg defended the fact that principal regulatory activity would be carried out by other primary sources: technology developers and social customs.⁴⁵

Indeed, Reidenberg's position was more consistent than the cyberlibertarian's stance, particularly when he related the function of social interactions on cyberspace and the power of developers to send regulatory messages while changing the network architecture.⁴⁶ It was well noted by Reidenberg that democratic values and the "common good" are directly dependent on some kind of network control that should be provided by different actors.⁴⁷ What cyberpaternalists forgot from the start was the density and the dynamism of the multiple simultaneous interactions among stakeholders.

Conclusion

Cyberspace has spawned a new public arena of

Internet Regulation and Data Protection, continued

deliberation, and its regulation is essential to preserve democratic values and choices. Instead of mere prohibition, regulation means transforming the reality to promote the environmental conditions for the development of society. Thus, it is almost impossible to ignore society's demands for new products and services like Uber, Airbnb, and Spotify. The disruption, convergence, and digitization processes are happening with or without the state's approval, and the development of civil society will most likely be better guided if the regulation is organized conjointly between the state and individuals, instead of by cyberpaternalistic verticalism or cyberlibertarian anarchy. If the state were to limit its participation in this process by simply prohibiting or allowing innovative products and services, society would through market, social norms, and architecture overwhelm the state's legislation in order to secure the viability of cyberspace's creativity and innovation.

Cyberpaternalism ignores the huge power that non-state users have on the Internet, or even the fact that Internet culture is emerging and becoming more and more complex. This, in the end, also affects user and governmental behavior inside and outside the Internet.

States must understand that regulation can be achieved in various ways, and not just by law. Indeed, states should also act through architecture, dealing directly with the code. Obviously, such interferences must be made legitimate by the appropriate mechanisms, but the necessity for governmental presence in coding is clear. Some countries have acted by blocking and filtering lists.⁴⁸ One clear sign of this in Brazil is the city of Curitiba, the capital of the state of Paraná, which took the initiative of adapting to Internet culture by creating a Facebook page and using humorous memes and current Internet jokes to communicate messages related to public policy on health, environment, and other issues of public interest and even to increase its own legitimacy as a democratic government.⁴⁹ It is clear that there is no perfect vertical regulation exerted from the state onto its citizens, especially in the civil law countries where the legislative branch is always behind technology and

information. In fact, curiously enough, the adaptive initiative of Curitiba was noticed by citizens of other Brazilian states, thousands of miles away, and they pushed for such adaptations in their own cities.

In summary, it is safe to conclude that the Internet has led to strong readapted processes of our model of state. The Internet has multiplied drastically communicative media and information dissemination. This process has engaged in the virtuous (or vicious, depending on point of view) cycle of technical development and communication expansion. Information is flowing in unprecedented rates, quantities, and forms. This has direct impact in all aspects of society, for reasons abovementioned. In this scenario, it is essential for the state to comprehend this new reality, despite its cumbersome bureaucracy, and to adapt in order to continue to represent its citizens and properly regulate this extended environment of society. Mere binary prohibition/allowance is a failed form of regulation, and interactive presence is the only way to obtain legitimacy and effectiveness in the digital environment.



Thiago Luís Santos Sombra is a lawyer, an arbitrator, a private law professor at the University of Brasilia (UnB), a visiting researcher at the London School of Economics-LSE, a former state attorney at the Brazilian Supreme Court, and a former clerk at the Superior Court of Justice.

Endnotes

- 1 David R. Johnson & David Post, *Law and borders: the rise of law in cyberspace*, 48 *STANFORD LAW REV.* 1367 (1995).
- 2 Lawrence Lessig, *CODE VERSION 2.0 AND OTHER LAWS OF CYBERSPACE* 27 (2006).
- 3 John Perry Barlow, *The next economy of ideas: selling wine without bottles on the global net*, 8 *WIRED*, 5 (2000).
- 4 Ronald Dworkin, *TAKING RIGHTS SERIOUSLY* 76 (2008).
- 5 Jon Berkeley, *The trust machine*, *THE ECONOMIST*, 2015, <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine> (last visited 2 Nov. 2015).
- 6 Benkler, *supra* note 5 at 15.
- 7 Manuel Castells, *THE RISE OF THE NETWORK SOCIETY: THE INFORMATION AGE: ECONOMY, SOCIETY, AND CULTURE* 23 (2011).
- 8 Barlow, *supra* note 8 at 10.

Internet Regulation and Data Protection, continued

- 9 Andrew D. Murray, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY 4 (2013).
- 10 Thomas Jefferson, *Thomas Jefferson's letter to Isaac McPherson: Article 1, Section 8, Clause 8*. THE FOUNDERS' CONSTITUTION (1813), http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html (last visited 1 Aug. 2015).
- 11 Benkler, *supra* note 5 at 25.
- 12 Murray, *supra* note 14 at 12.
- 13 *Id.* at 26.
- 14 Barlow, *supra* note 8.
- 15 Andrew Murray, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 22 (2007).
- 16 Tim Berners-Lee, *WWW: past, present, and future*, 29 COMPUTER 69–77, 74 (1996).
- 17 Peter Diamandis, THESE MULTI-BILLION DOLLAR INDUSTRIES ARE RIPE FOR DISRUPTION THIS DECADE (2015), <https://www.linkedin.com/pulse/ripe-disruption-part-2-peter-diamandis> (last visited 27 Oct. 2015); Michael Rundle, *Government outlines "smartphone state," via Uber and blockchain*, WIRED UK (2015), <http://www.wired.co.uk/news/archive/2015-09/22/matt-hancock-mp-interview-digital-government> (last visited 27 Oct. 2015).
- 18 John Perry Barlow, *A declaration of the independence of cyberspace*, 10 WIRED (1996).
- 19 Gian Volpicelli & Alex Pentland: *Big data will help us hold governments accountable*, WIRED UK (2015), <http://www.wired.co.uk/news/archive/2015-10/15/alex-pentland-wired-2015> (last visited 27 Oct. 2015).
- 20 Benkler, *supra* note 5 at 137.
- 21 Barlow, *supra* note 23.
- 22 Murray, *supra* note 14 at 75–76.
- 23 Rafael Barifouse, *Mais da metade das capitais do Brasil já têm projetos de lei contra o Uber*, BBC BRASIL, 10 September 2015, http://www.bbc.com/portuguese/noticias/2015/09/150908_uber_projetos_de_lei_rb (last visited 27 Oct. 2015).
- 24 Andy Greenberg, *Mapping how Tor's anonymity network spread around the world*, WIRED UK, 2015, <http://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/> (last visited 27 Oct. 2015).
- 25 The Crown Prosecution Service, INDECENT PHOTOGRAPHS OF CHILDREN: LEGAL GUIDANCE THE CROWN PROSECUTION SERVICE (1997), http://www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/ (last visited 27 Oct. 2015); Liat Clark, *Minister Joanna Shields to combat online child abuse and terrorism*, WIRED UK, 2015, <http://www.wired.co.uk/news/archive/2015-05/19/joanna-shields-new-internet-safety-minister> (last visited 27 Oct. 2015).
- 26 Kevin Simpson, *How a cyberbullying law in Colorado was tweaked to be more effective*, DENVER POST, 14 July 2015, http://www.denverpost.com/news/ci_28479145/cyberbullying-tweaks-colorado-law-can-impose-fines-jail (last visited 4 Aug. 2015).
- 27 Lizzie Dearden, *People who spread revenge porn will at last face justice*, THE INDEPENDENT, 13 April 2015, <http://www.independent.co.uk/news/uk/home-news/revenge-porn-illegal-in-england-and-wales-under-new-law-bringing-in-two-year-prison-terms-10173524.html> (last visited 27 Oct. 2015).
- 28 Andrea Peterson, *Could hackers take down a city?*, THE WASHINGTON POST, 18 August 2015, <https://www.washingtonpost.com/news/the-switch/wp/2015/08/18/could-hackers-take-down-a-city/> (last visited 27 Oct. 2015).
- 29 Abigail Tracy, *While The Supreme Court Hesitates On Warrantless Cell Location Data Collection, Your Privacy Remains At Risk*, FORBES, 2015, <http://www.forbes.com/sites/abigailtracy/2015/10/16/while-the-supreme-court-hesitates-on-warrantless-cell-location-data-collection-your-privacy-remains-at-risk/> (last visited 27 Oct. 2015).
- 30 Isabela Palhares, *Celular é principal forma de acesso à internet pelos jovens - Educação*, O ESTADO DE SÃO PAULO, 28 July 2015, <http://educacao.estadao.com.br/noticias/geral,celular-e-principal-forma-de-acesso-a-internet-pelos-jovens-brasileiros,1733869> (last visited 27 Oct. 2015).
- 31 BBC News, FINANCE FIRMS TARGETED BY CYBER EXTORTION GANG BBC NEWS (2015), <http://www.bbc.com/news/technology-34205258> (last visited 28 Oct. 2015).
- 32 Greenberg, *supra* note 30.
- 33 Cass Sunstein, REPUBLIC.COM 2.0 25 (2 ed. 2009).
- 34 Volpicelli, *supra* note 24.
- 35 Suzanne Dovi, POLITICAL REPRESENTATION THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., Spring 2014 ed. 2014), <http://plato.stanford.edu/archives/spr2014/entries/political-representation/> (last visited 9 Oct. 2015).
- 36 Benkler, *Supra* Note 5 At 241; Lessig, *Supra* Note 7 At 28.
- 37 Jacqueline Jones, *France top court rules surveillance law constitutional*, JURIST (2015), <http://jurist.org/paperchase/2015/07/france-top-court-rules-surveillance-law-constitutional.php> (last visited 1 Aug. 2015).
- 38 Josh Taylor, RIGHTS HOLDERS COULD GET SITES BLOCKED WITHOUT EVIDENCE (2015), <http://www.zdnet.com/article/rights-holders-could-get-sites-blocked-without-evidence/> (last visited 4 Aug. 2015).
- 39 Patrick Robinson, *London reveals new policy on home sharing*, THE AIRBNB PUBLIC POLICY BLOG (2015), <http://publicpolicy.airbnb.com/london-reveals-new-policy-home-sharing/> (last visited 2 Aug. 2015).
- 40 Joel R. Reidenberg, *Lex Informatica: The formulation of information policy rules through technology*, 76 TEX REV 553, 554–555 (1997).
- 41 Murray, *supra* note 14 at 60.
- 42 Reidenberg, *supra* note 46 at 576–577; Andrew D. Murray, *Nodes and gravity in virtual space*, 5 LEGISPRUDENCE 195–221, 3–4 (2011).
- 43 Reidenberg, *supra* note 46 at 581.
- 44 The best examples are the statute that passed in Colorado criminalizing cyberbullying and the French HADOPI law. Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), GRADUATED RESPONSE HADOPI LAW FOR THE RIGHTS PROTECTION HADOPI (2010), <http://www.hadopi.fr/en/haute-autorite/about-hadopi> (last visited 4 Aug. 2015); Simpson, *supra* note 32.
- 45 Reidenberg, *supra* note 46 at 76.
- 46 *Id.* at 588.; Murray, *supra* note 48 at 5.
- 47 Sunstein, *supra* note 39 at 32.
- 48 Sophie Curtis, *BT forces porn filter choice*, THE TELEGRAPH, 16 December 2013, <http://www.telegraph.co.uk/technology/internet-security/10520537/BT-forces-porn-filter-choice.html> (last visited 28 Oct. 2015); Murray, *supra* note 14 at 72.
- 49 Marina Pinhoni, *Curitiba é hoje cidade mais engraçada do Brasil*, Online REVISTA EXAME, 2014, <http://exame.abril.com.br/brasil/noticias/curitiba-e-hoje-cidade-mais-engracada-do-brasil-veja-razao> (last visited 28 Oct. 2015).



2017

LAUNCH

NEW FASTCASE 7

FLY THROUGH YOUR LEGAL RESEARCH WITH THE NEWEST VERSION OF THE WORLD'S MOST VISUAL SEARCH PLATFORM. RESERVE YOUR SEAT TODAY AT 866-773-2782

LEARN MORE AT:
WWW.FLORIDABAR.ORG

DOWNLOAD THE APP



THE FLORIDA BAR



comes to the U.S. Department of Homeland Security, think again.

Nevertheless, the U.S. Congress and CBP want to expand the number of people who become members of Global Entry. When the Committee on Appropriations for the U.S. House of Representatives made its 2015 annual appropriations for the U.S. Department of Homeland Security, including CBP, it made special mention of the Global Entry program. It stated, in relevant part:

The Committee is pleased to see the Global Entry program transition from a successful pilot to a permanent trusted traveler program. The Committee encourages CBP to continue to increase individual enrollment as well as the number of nations eligible to participate in the program. This will allow greater numbers of low risk travelers to efficiently move through security screening and give CBP personnel the ability to put greater focus on higher-risk travelers . . .

If an applicant believes he or she is exactly the type of low-risk international traveler that the members of the Committee on Appropriations were contemplating in funding the Global Entry program, the applicant should file a request for reconsideration with CBP.

Please note that being admitted into Global Entry is a privilege, not a right. As explained in the case of *Roberts v. Napolitano*, 792 F. Supp. 2d 67, 73 (D.D.C. 2011):

The Global Entry program was authorized by the Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter "IRTPA"). See 8 U.S.C. § 1365b(k). The IRTPA instructs the Secretary of Homeland Security to "establish an international registered traveler program" in order to "expedite the screening and processing of international travelers, including United States Citizens and residents, who enter and exit the United States." 8 U.S.C. § 1365b(k)(3)(A). The Secretary was further instructed to "initiate a rulemaking to establish the program [and] criteria for participation," and ensure that the program "includes as many participants as practicable by . . . providing applicants with clear and consistent eligibility guidelines." 8 U.S.C. § 1365b(k)(3)(C), (E).

The applicant gets one chance to appeal a denial, and a member gets one chance to challenge revocation of membership in Global Entry. There is no judge, no hearing, no discovery, no face to face meeting, or even a telephone call to the deciding official at CBP. As stated above, CBP has absolute discretion to grant

Think Outside the Box, from page 31

Verification Program (ASVVP), designed to complement the Department of Homeland Security's antifraud efforts.¹³ Initially, the ASVVP only performed H-1B site inspections; however, as of fiscal year 2014, the program has been expanded to cover L-1 site visits.¹⁴ Under the program, site visits are conducted by the Fraud Detection and National Security directorate (FDNS) of the USCIS. During an FDNS site visit, the inspector is typically charged with verifying the existence of the employer, the validity of the information the employer provided in the H-1B or L-1 petition, and whether the foreign national is working in compliance with the terms of the H-1B or L-1 approval. It is interesting to note that the FDNS site visits occur post adjudication (approval) of the H-1B and L-1 petitions by the USCIS.¹⁵

Specifically, the H-1B numerical cap comprises 65,000 H-1B visas per fiscal year and an additional 20,000 per year reserved for foreign national beneficiaries who have earned a U.S. master's degree or higher.¹⁶ Based on free trade agreements entered into by the United States with Singapore and Chile, from the 65,000 H-1B visas available per fiscal year, there are 1,400 H-1B's, called H-1B1's, reserved for professionals from Chile and 5,400 for professionals from Singapore, per fiscal year.¹⁷ Because of the numerical cap and the high demand for H-1B workers in the past several years, the USCIS has relied upon a computer-generated random selection process to select, from the large pool of petitions received, only enough petitions to meet the numerical cap.¹⁸ During both 2015 and 2016, only 36%

of the petitions filed were selected for review.¹⁹ Clearly, the numbers reflect that the H-1B process has become one based on luck, with worsening odds each year.

On the congressional side, emboldened by the results of the BFCa and subsequent programs instituted by the USCIS such as VIBE and the ASVVP, Iowa Senator Chuck Grassley spearheaded the initiative to eliminate perceived abuses



Perhaps the biggest challenge to employers using the H-1B program is the H-1B annual quota, also known as the "numerical cap." The majority of employers that file H-1B petitions are subject to an annual quota. In recent years, petitioner employers have faced the additional hurdle of not having their petitions adjudicated by the USCIS due to the numerical limitation on the H-1B

in the H-1B and L-1 classifications. In so doing, he introduced the H-1B and L-1 Visa Reform Act of 2013²⁰ and subsequently, the H-1B and L-1 Visa Reform Act of 2015.²¹ This legislation called for substantive revisions to the H-1B and L-1 classifications, including reforms to increase enforcement and modify wage requirements. Though Senator Grassley's proposed legislation in 2013

Think Outside the Box, continued

and 2015 did not move past the introductory stage in the Senate, under the new administration, which is led by a president whose successful campaign focused on promises that he would make substantive changes to our current immigration system, similar proposals may prove successful. As such, U.S. employers can no longer ignore the writing on the wall, as there is a much greater possibility under President Trump's administration that certain changes to our employment-based visa system may be made.

The Current Administration: Another Brick in the Wall

On President Trump's first day in office, Senator Grassley introduced the H-1B and L-1 Visa Reform Act of 2017.²² An identical bill was introduced in the House of Representatives, titled H-1B and L-1 Visa Reform Act of 2017.²³ These bills seek to impose among other requirements: the establishment of an H-1B visa allocation system, composed of eight tiers, with first priority reserved for foreign nationals who have earned an advanced degree in a field of science, technology, engineering, or mathematics (STEM) from a U.S. institution of higher education and second priority given to U.S. employers who will pay the H-1B beneficiary the median wage for the highest skill level in the occupational classification in the area of intended employment; the reduction of the period of authorized admission for an H-1B nonimmigrant from six to three years with specific standards for extension; and the requirement that no employer may replace a U.S. worker with an L-1 worker.²⁴

Within the executive branch, the first indication of President Trump's focus on reforms to employment-based immigration was revealed through a leaked January 2017 draft Executive Order, titled *Executive Order on Protecting American Jobs and Workers by Strengthening the Integrity of Foreign Worker Visa Programs*. The draft Executive Order broadly proposes the "review of all regulations that allow foreign nationals to work in the United States" [to] determine which of those regulations violate the immigration laws or are

otherwise not in the national interest and should be rescinded, and propose for notice and comment a rule to rescind or modify such regulations" (emphasis added). The draft Executive Order also directs the secretary of the Department of Homeland Security, among other measures, to "develop a plan to expand the site-visit program within two years to cover all employment-based visa programs."

In light of likely changes to the commonly used H-1B and L-1 classifications, there is a need for U.S. employers to stay abreast of this developing area. Moreover, exploration of alternative visa classifications, in conjunction with business immigration counsel, is merited. As will be discussed below, the E-2 and O-1 classifications are often welcome solutions for employers and should be explored during these uncertain times.

Navigating the Trends by "Thinking Outside the Box"

E-2 Treaty Investor Visa – A Useful Strategy for Treaty Nationals in Executive/Supervisory/Essential Employee Positions

The Treaty Investor E-2 classification may prove a viable option for U.S. employers classified as treaty investors to employ foreign nationals possessing the nationality of the treaty country in executive or supervisory roles, or in capacities requiring essential skills. The E-2 classification is for nationals of countries with which the United States maintains treaties of commerce and navigation.²⁵ To date, eighty countries have qualifying treaties with the United States for purposes of E-2 classification.²⁶

The E-2 visa is commonly associated with a visa applicant who is coming to the United States to develop and direct the operations of an enterprise in which the applicant has invested or is actively in the process of investing a substantial amount of capital.²⁷ A common misconception is that the E-2 classification is reserved only for individual investors. Many are surprised to learn that an E-2 visa applicant may also be a prospective employee if he or she has the same nationality as the principal investor employer, and is in or is coming to the United States to engage in duties of an executive or

Think Outside the Box, continued

supervisory character, or, if employed in a lesser capacity, the employee has special qualifications that make his or her services essential to the efficient operation of the U.S. enterprise.²⁸ It is important to note that an E-2 principal investor employer may be an individual or a business.²⁹

The requirements for an E-2 visa include the following: (1) a qualifying treaty of commerce and navigation must exist between the United States and a foreign state (treaty country) in order for the E visa classification to be accorded to nationals of that foreign state;³⁰ (2) an individual and/or business must possess the nationality of the treaty country;³¹ (3) an applicant must have invested or must be actively in the process of investing in an enterprise;³² (4) the enterprise must be a real and operating commercial enterprise;³³ (5) the applicant's investment must be substantial;³⁴ (6) the investment must be more than a marginal one solely for earning a living for the treaty investor and his or her family;³⁵ (7) the principal applicant must be in a position to "develop and direct" the enterprise;³⁶ (8) the applicant, if an employee, must be destined to an executive/supervisory position or possess skills essential to the enterprise's operations in the United States;³⁷ and (9) the applicant must intend to depart the United States when the E-2 status terminates.³⁸

The E-2 application process does not require pre-approval from the USCIS as is typically required for L-1 and H-1B petitions, as an E-2 visa applicant may apply directly at a U.S. Embassy or Consulate abroad. It is important to note that each U.S. Embassy or Consulate has its own set of specific instructions on the application process. As an example, the U.S. Embassy in Madrid, Spain, requires first-time E-2 visa applicants to mail hard copies of their application at least two weeks before scheduling a consular interview, and the application package cannot exceed fifty pages.³⁹ In contrast, the U.S. Embassy in Brasília and the U.S. Consulates in São Paulo, Rio de Janeiro, and Recife require applicants to schedule an appointment at one of the Applicant Service Centers (ASC) to submit required biometric information and the E-2 Visa application package, which is limited

to 100 pages.⁴⁰ While the United States and Brazil do not maintain a treaty of commerce and navigation, Brazilian citizens who also hold dual citizenship from an E-2 treaty country, such as Italy, Japan, or Paraguay, may apply for an E-2 visa at a U.S. Consulate in Brazil.⁴¹ The period of validity of the E visa varies between countries based upon a reciprocity schedule. The initial period of admission is two years and may be renewed indefinitely for an executive, supervisor, or principal investor, as long as the individual with an E visa or E status is still necessary to supervise or direct and develop the enterprise. Employees with essential skills will be subject to greater scrutiny with respect to initial entry and renewal.

The E-2 classification permits spouses and minor unmarried children under 21 to accompany or follow to join the E-2 beneficiary.⁴² The nationality of the spouse or the child is irrelevant as to whether he or she qualifies for the E-2 derivative benefit.⁴³ Further, the E-2 spouse is eligible to apply for work authorization in the United States.⁴⁴ Although the E-2 may be renewed indefinitely, the classification requires that the E-2 employee and his or her family maintain the intent to depart the United States upon the expiration or termination of the status.⁴⁵ An E-2 nonimmigrant may file for permanent residence through different legal strategies, but certain considerations apply; such strategies and considerations are beyond the scope of this article.

O-1 Extraordinary Ability Visa Classification – Employing the Best and the Brightest

The O-1 visa classification is for individuals who possess extraordinary ability in the sciences, arts, education, business, or athletics, or who have a demonstrated record of extraordinary achievement in the motion picture or television industry and have been recognized nationally or internationally for those achievements. Many U.S. employers believe that the O-1 classification is reserved only for Oscar and Grammy winning entertainers and sports stars; however, a mere mortal, such as a businessperson whose extraordinary ability in business has been demonstrated by sustained national

Think Outside the Box, continued

and international acclaim⁴⁶ and is one of the small percentage who has risen to the very top of the field of endeavor, may also eligible for the O-1 classification.⁴⁷

In order to qualify for O-1 classification in the field of business, a businessperson may prove his or her extraordinary ability in business, and specifically his or her sustained national and international acclaim by documenting at least three of the following criteria:⁴⁸

- Documentation of the alien's receipt of nationally or internationally recognized prizes or awards for excellence in the field of endeavor;
- Documentation of the alien's membership in associations in the field for which classification is sought, which require outstanding achievements of

their members, as judged by recognized national or international experts in their disciplines or fields;

- Published material in professional or major trade publications or major media about the alien, relating to the alien's work in the field for which classification is sought, which shall include the title, date, and author of such published material, and any necessary translation;
- Evidence of the alien's participation on a panel, or individually, as a judge of the work of others in the same or in an allied field of specialization to the one for which classification is sought;
- Evidence of the alien's original scientific, scholarly, or business-related contributions of major significance in the field;



U.S. President Donald Trump executes Executive Order on immigration issues in January 2016 (Chip Somodevilla/Getty Images).

Think Outside the Box, continued

- Evidence of the alien's authorship of scholarly articles in the field, in professional journals, or in other major media;
- Evidence that the alien has been employed in a critical or essential capacity for organizations and establishments that have a distinguished reputation; and
- Evidence that the alien has either commanded a high salary or will command a high salary or other remuneration for services, evidenced by contracts or other reliable evidence.

If the criteria above do not readily apply to the beneficiary's occupation, the petitioner may submit comparable evidence in order to establish the beneficiary's eligibility.⁴⁹

Some of the most commonly met criteria for O-1 classification in the field of business are that the foreign national has played a critical or essential capacity for organizations and establishments that have a distinguished reputation; evidence that he or she has participated on a panel, or individually, as a judge of the work of others; and that he or she has commanded a high salary. While the O-1 classification is a temporary visa requiring nonimmigrant intent, it may be renewed indefinitely as long as the person continues working in his or her field of extraordinary ability. It should be noted that there is no requirement that the position in the United States require a person of O-1 caliber.⁵⁰ O-1's are not eligible for self-employment, and the O-1 process entails the filing of the O-1 petition with the USCIS and such filing must establish the employer's and the prospective employee's eligibility for the classification.

The O-1 is typically approved for three years, and extensions are granted in one-year increments for the same event.⁵¹ An O-1 petition filed by a new employer or for a new position with the same employer may be considered a "new" event, and may be extended for another full three years.⁵² Spouses and unmarried children under 21 are eligible to accompany or follow to join the principal O-1 applicant, and are granted the O-3 visa classification.⁵³ The O-3 visa classification authorizes

spouses and unmarried children under 21 of the O-1 principal to live and study in the United States, but O-3 status does not allow for employment authorization.⁵⁴ Assuming approval by the USCIS of the O-1 petition, prior to commencing employment under such status, the foreign national, unless eligible for a waiver of the visa requirement, must first apply for and be issued a visa by a U.S. Consulate abroad.

In addition to being an effective visa classification for U.S. employers to hire the "best and the brightest" on a temporary basis, the O-1 classification allows for an upgrade to "permanent residence" or in other words, for a "green card" under the Employment-Based First Preference category for priority workers, commonly referred to as the EB-1.⁵⁵ Unlike in the O-1 context, self-employment/self-petition is an option for the EB-1, as no employer or specific offer of employment is required. The foreign national must intend to pursue work in the United States in the area of expertise, and his or her entry must substantially benefit prospectively the United States.⁵⁶ Although approval of an O-1 petition is not dispositive and does not compel the USCIS to approve the EB-1, the O-1 petition can provide a solid basis for an EB-1, assuming the employee decides to file for permanent residence at some point in the future.

Conclusion

In the recent past, standalone immigration legislation targeted at combating the perceived abuses in the H-1B and L-1 visa classifications has been unsuccessful. In today's new era of broadened immigration enforcement, similar efforts may prove successful. In the ever-evolving area of U.S. employment-based immigration, U.S. employers are well advised to keep abreast of new developments, to look beyond the heavily relied upon Specialty Occupation Worker H-1B and Intracompany Transferee L-1 classifications, and to explore alternative visa classifications, such as the Treaty Investor E-2 and the Extraordinary Ability O-1, as a strategy that may prove effective to fill critical employment needs.

Think Outside the Box, continued



Mariana R. Ribeiro is a partner in Gunster's Immigration Practice Group. Gunster is a full-service commercial law firm with more than 180 attorneys collaborating across 18 practice areas, including employment-based immigration. A Chambers recognized attorney, Ms. Ribeiro's primary practice

focuses on multifaceted and complex employment-based nonimmigrant and immigrant visa matters. A native of Brazil, she is fluent in both Portuguese and Spanish and frequently handles cross-border matters that are conducted and documented exclusively in Portuguese.



Beatriz E. Osorio is an attorney in Gunster's Immigration Practice Group. She counsels employers in a variety of industries, including finance and banking, health care, and technology, regarding policies, required documentation, and procedures related to sponsoring foreign nationals and

compliance with U.S. immigration laws. A Colombian native, she is bilingual in Spanish and English.

Endnotes

1 Exec. Order No. 13768, Enhancing Public Safety in the Interior of the United States, 82 Fed. Reg. 8799 (25 January 2017); Exec. Order No. 13767, Border Security and Immigration Enforcement Improvements, 82 Fed. Reg. 8793 (25 January 2017); Exec. Order No. 13769, Protecting the Nation from Foreign Terrorist Entry into the United States, 82 Fed. Reg. 8977 (25 January 2017); and Exec. Order No. 13780, Protecting the Nation from Foreign Terrorist Entry into the United States, 82 Fed. Reg. 13209 (6 March 2007).

2 INA § 101(a)(15)(H)(i)(b); 8 C.F.R. § 214.2(h)(1)(ii)(B)(1).

3 8 C.F.R. § 214.2(h)(4)(iii)(A).

4 8 C.F.R. § 214.2(h)(4)(i)(B).

5 22 C.F.R. § 731.

6 22 C.F.R. § 732.

7 22 C.F.R. § 733.

8 22 C.F.R. § 734.

9 INA § 101(a)(15)(L); 8 C.F.R. § 214.2(l)(1)(i).

10 U.S. Citizenship and Immigration Services, FDNS, H-1B Benefit Fraud & Compliance Assessment (2008).

11 Memo, Neufeld, Acting Assoc. Director, Domestic Operations, H-1B Anti-Fraud Initiatives – Internal Guidance and Procedures in Response to Findings Revealed in H-11B Benefit Fraud and Compliance Assessment, HQ 70/35.2 (31 October 2008).

12 [https://www.uscis.gov/working-united-states/information-](https://www.uscis.gov/working-united-states/information-employers-employees/employer-information/vibe/validation-instrument-business-enterprises-vibe-program)

[employers-employees/employer-information/vibe/validation-instrument-business-enterprises-vibe-program](https://www.uscis.gov/working-united-states/information-employers-employees/employer-information/vibe/validation-instrument-business-enterprises-vibe-program).

13 Administrative Site Visit and Verification Program, <https://www.uscis.gov/about-us/directorates-and-program-offices/fraud-detection-and-national-security/administrative-site-visit-and-verification-program>.

14 *Id.*

15 *Id.*

16 INA §§ 214(g)(1)(A), 214(g)(8)(B)(iv), 8 USC §§ 1184 (g)(1)(A), 1184 (g)(8)(B)(iv); PL 108-77 and 108-78.

17 *Id.*

18 <https://www.uscis.gov/news/news-releases/uscis-reaches-fy-2016-h-1b-cap>; and <https://www.uscis.gov/news/news-releases/uscis-reaches-fy-2017-h-1b-cap>.

19 *Id.*

20 H-1B and L-1 Visa Reform Act of 2013, S.600, 113th Cong. (2013).

21 H-1B and L-1 Visa Reform Act of 2015, S.2266, 114th Cong. (2015).

22 H-1B and L-1 Visa Reform Acts of 2017, S. 180, 115th Cong. (2017).

23 H-1B and L-1 Visa Reform Acts of 2017, H.R. 1303, S. 115th Cong. (2017).

24 *Id.*

25 INA § 101 (a)(15)(E)(ii).

26 U.S. Dep't of St. Bureau of Consular Affairs, <https://travel.state.gov/content/visas/en/fees/treaty.html>.

27 INA § 101(a)(15)(E)(ii); 8 C.F.R. § 214.2 (e)(2).

28 8 C.F.R. § 214.2 (e)(3).

29 9 FAM 402.9-4(B).

30 9 FAM 402.9-4 (A).

31 9 FAM 402.9-4 (B).

32 9 FAM 402.9-6 (B).

33 9 FAM 402.9-6 (C).

34 9 FAM 402.9-6 (D).

35 9 FAM 402.9-6 (E).

36 9 FAM 402.9-6 (F).

37 9 FAM 402.9-7.

38 9 FAM 402.9-4 (C).

39 https://madrid.usembassy.gov/visas/treaty2/new_e2_cases.html.

40 https://br.usembassy.gov/visas/treaty-trader-investor-e1e2-visas/?_ga=1.79183764.1696973994.1420649862.

41 *Id.*

42 8 C.F.R. § 214.2 (e)(4).

43 *Id.*

44 INA § 214(e)(6).

45 8 C.F.R. § 214.2 (e)(5).

46 8 C.F.R. § 214.2(o)(1)(ii)(A)(1).

47 8 C.F.R. § 214.2(o)(3)(ii).

48 8 C.F.R. § 214.2(o)(3)(iii).

49 *Id.*

50 8 C.F.R. § 214.2(o)(1)(ii)(A)(1) and (2).

51 8 C.F.R. § 214.2(o)(6)(iii)(A) and 8 C.F.R. § 214.2(o)(12)(ii).

52 8 C.F.R. § 214.2(o)(3).

53 8 C.F.R. § 214.2(o)(6)(iv).

54 *Id.*

55 INA § 203(b)(1)(A).

56 INA § 204(a)(1)(E); 8 C.F.R. § 204.5(h)(1).

The Florida Bar
651 East Jefferson Street
Tallahassee, FL 32399-2300

FIRST CLASS
U.S. POSTAGE
PAID
TALLAHASSEE, FL
Permit No. 43

INTERNATIONAL ARBITRATORS.COM

A Full Service International Arbitration Law Firm

International Arbitration is Our Domain.

Investment Treaty | Business | Commercial

Contact: Santiago A. Cueto
4000 Ponce de Leon Blvd., Suite 470
Coral Gables, FL 33146 | +1 305.777.0377
Scueto@InternationalArbitrators.com

Visit www.InternationalArbitrators.com

InternationalArbitrators.Com is a division of
Cueto Law Group, P.L. ©Cueto Law Group 2015. All rights reserved.

