A New Era for the International Law Section
SEE INSIDE FOR THE MANY WAYS YOU CAN GET INVOLVED

California Now Open for Business in International Arbitration
By Howard B. Miller, p. 11

Thief in the Night: The Invasive Nature of Home Internet of Things and Its Attempt to Silently Shift Rules of Personal Data Ownership
By Celine Melanie A. Dee, p. 31

Steel, Tariffs and National Security Under the Trump Administration
By Robert Bowen, p. 53
The California International Law Journal is published by the International Law Section (ILS) of the California Lawyers Association (CLA). The Journal’s mission is to include a diverse array of practical articles relating to topics and issues in international law and to showcase cutting-edge research on important and unique subjects in the field. We strive to provide in-depth coverage and analysis for professionals, as well as to assist in the development and exchange of academic work. In addition, we serve the ILS, CLA and international law community as a whole by connecting practitioners, legislators, judicial officers and academics in the United States and abroad, and by promoting conferences, symposia, practicums, webinars, exchanges and education related to international legal issues.

Any lawyer in the United States or any other country, as well as any law student, may submit articles to the Journal. Those in other professions are welcome to submit articles relating to international law as well. We encourage a diverse authorship with diverse viewpoints, and are committed to publishing content in a wide variety of areas, such as business, trade, intellectual property, technology, immigration/asylum, criminal justice, human rights, comparative law and the intersection of law and other disciplines.

The Journal is accepting submissions on an ongoing basis. Please send proposed articles directly to Catherine L. Carlisle and/or Hera U. Smith at ils@calawyers.org.

ILS Membership Includes a Subscription to The California International Law Journal.

The California International Law Journal Editorial Team

Executive Editorial Board
Catherine L. Carlisle, Editor-in-Chief
Hera U. Smith, Managing Editor
Robert Pimm, Executive Editor
Melis Biskin, Articles Editor
Charles Kaufman, Articles Editor
Jessica Vapnek, Articles Editor
Alan Tse, Production Editor
Payal Sinha, Outreach Editor
Natalia C. Aranovich, Marketing Director

Advisory Board
Jeffery J. Daar
Alexandra Darrabé
William Tolín Gay
Emilio Varanini

International Advisory Board
Sophia Harris (France)
Thérèse Keelaghan (France)

General Editorial Board
Robert Bowen
Augustin Ceballos
Lavonne Lawson
Courtney McCausland
Dennis T. Rice

The Journal invites foreign bar friends to join our International Advisory Board and ILS members to join our General Editorial Board.
If you are interested, please contact Catherine L. Carlisle and/or Hera U. Smith at ils@calawyers.org.
It is my great honor to serve as the first Editor-in-Chief of *The California International Law Journal* following the formation of the nonprofit California Lawyers Association (CLA) and the International Law Section’s (ILS) move to the CLA.

This transition year has afforded the Journal and the ILS as a whole the opportunity to revisit our goals and reinvigorate our approach to serving our community. Our ILS Co-Chairs Alexandra Darraby and Michael Newman will highlight in this Edition the ILS’s significant accomplishments in making our Section even more successful and in facilitating the transition of all the Sections to the CLA. At the Journal, thanks to our Editorial Board and the generous support of the ILS Co-Chairs, we are proud to have already achieved the following:

- Developed initiatives to improve the relevance, diversity and quality of our content to ensure that our publication meets our readers’ needs—both in California, the U.S. as a whole and across the globe;
- Increased our outreach to Section members, international partners and national and international professional organizations and law schools to encourage article submissions that are truly representative of and helpful to our readership;
- Appointed a full **Executive Editorial Board** to assist with content development, outreach, advertising and sponsorship opportunities;
- Created an **International Advisory Board**—comprised of representatives from bar associations with whom we have friendship agreements—to ensure that our foreign partners have a voice in making the Journal truly international;
- Added experienced international practitioners and former Journal Editors-in-Chief to our Advisory Board;
- Implemented a complete redesign of the Journal with our partners at Sublime Designs to both modernize its look and feel and make it more accessible; and
- Committed ourselves to promoting and facilitating an open and ongoing dialogue with our authors and readers so that we continue to meet your needs.

*The California International Law Journal* has been an integral part of the ILS for almost three decades. Originally titled *The California International Practitioner*, the Journal was founded under the leadership of Robert E. Lutz, Professor of Law at Southwestern Law School. Aided by Professor Lutz’s truly remarkable expertise—as one of the foremost authorities on international public and private law, the founder and leader of many prestigious international legal organizations and publications, a frequent advisor to entities such as the U.S. State Department and the World Trade Organization, a renowned arbitrator and practitioner and the recipient of the ILS’s Fourth Annual Warren M. Christopher International Lawyer of the Year Award—the Journal immediately became a well-respected publication in the international law community.

The Journal’s editors throughout the years have since built on this foundation to make the Journal what it is today. I want to take this opportunity to thank Professor Lutz for his crucial initial leadership, all of our prior editorial board members for their contributions and in particular my three direct predecessors, William K. Pao, Mark Danis and Emilio Varanini, who have each spent significant time and effort reviving and improving the Journal.

Of course, the strides we have made this year and our preparations for the year to come could not have been possible without the tireless work of our Editorial Board. All of the members of our inaugural (and all volunteer) Executive Editorial Board have
immediately and enthusiastically offered their assistance, their time and their important suggestions and perspectives. Special thanks to Hera Smith, our Managing Editor, for her hard work on all aspects of the Journal.

Finally, I want to thank all of our authors and readers for your contributions and support, especially during this transition. You are the reason we exist, and we hope to increasingly reflect your needs and interests in the years to come.

We want to encourage an open dialogue—so please don’t hesitate to contact us with any comments, questions, suggestions or submissions! Additionally, if you are interested in joining our General Editorial Board or International Advisory Board, we would welcome your participation and ideas! You may contact Catherine L. Carlisle and/or Hera U. Smith directly at ils@calawyers.org.

Thank you for your interest and support.

Cathy Carlisle
Editor-in-Chief

* Catherine (Cathy) Carlisle is an Attorney at Yukevich | Cavanaugh, a Los Angeles-based litigation boutique. She focuses on complex commercial litigation matters spanning a wide variety of subjects, and is experienced in international litigation and arbitration. Cathy graduated from Northwestern University Pritzker School of Law and practiced at several large, international law firms on both coasts prior to joining Yukevich | Cavanaugh. In addition to her law practice, Cathy is a Professor at University of California, Irvine School of Law, teaching pretrial advocacy, depositions and advanced litigation writing. She leads a yearly program at Southwestern Law School providing recent graduates with advanced litigation training.
t is our honor and privilege to serve as the first International Law Section Co-Chairs under the new California Lawyers Association.

We would like to take this opportunity to welcome to the ILS community new and renewing ILS Members, as well as members from Foreign Bar Associations with whom we have Friendship Agreements.

As many of you know, 2018 has been a year of many transitions. The California Lawyers Association (CLA), established this year, is a nonprofit, voluntary organization and the new home for all the Sections of the State Bar of California and the California Young Lawyers Association. It is a member-driven, mission-focused organization dedicated to the professional advancement of attorneys practicing in the State of California. The CLA’s extensive membership represents the vast diversity of California’s legal community and the various areas of law practiced throughout the State. The CLA is dedicated to promoting excellence, diversity and inclusion in the legal profession and fairness in the administration of justice and the rule of law.

The ILS is a growing and important Section-member of the CLA. The ILS is the authorized representative of the CLA to enter into Friendship Agreements with foreign bar associations that meet criteria developed by the Section. Friendship Agreements provide the international profile of CLA, and renew commitments of California and foreign counsel to concepts such as the rule of law, human dignity, mutual cooperation and objective norms in the practice and advocacy of law.

The ILS continues to perform this important function for lawyers in California under the CLA as it did under the State Bar. We are engaging in new and innovative ways to better serve our Section members and the California public and legal community in this new era.

This year the ILS joined all CLA Sections in developing and implementing policies and guidelines for the CLA. The ILS has been particularly involved in assisting with the transition, with the support and input of ILS members. While working with the CLA Board of Representatives and CLA staff to coordinate compliance and advocate for the unique international interests of the ILS within the CLA, the ILS Executive Committee actively reached out to members—new and old. Like the vintage Uncle Sam posters, “we want you.” If you are not yet a member of the CLA, join the CLA on the link below and mark the International Law Section as your home base in the organization.

We are proud of our dynamic ILS Executive Committee and our ILS CLA Board Representative, Brian Arbetter, who all worked together to accomplish so much in so little time, under tight deadlines and with limited resources. In its first six-month tenure, the all-volunteer ILS Executive Committee was able to accomplish the following:

- Successfully initiated broad-based CLA support of proposed legislation regarding international arbitration (SB 766) in the California Assembly, and worked with the CLA Director of Government Affairs to provide education about SB 766, which has passed and has been sent to the Governor for signature;
• Re-instituted the ILS Newsletter, reviving communications among ILS members and connecting members with ILS programs and events;

• Appointed a new Executive Editorial Board for the ILS’s well-respected publication, *The California International Law Journal*, including Editors and Managers to assist with content development, advertising and sponsorship, as well as to develop revenue opportunities;

• Maintained public engagement with international career programs in California law schools, including UCLA, USC and Chapman;

• Expanded cross-border cooperation with Foreign Bars, drafted and adopted procedures and criteria for establishing relationships with Foreign Bars and created a new form of Friendship Agreement within the guidelines of the new CLA;

• Developed additional ILS Foreign Bar Friends in Asia and Europe and participated in international conferences hosted by our Foreign Bar Friends;

• Grew our membership by 30%;

• Continued the successful intra-bar informal ILS networking “mixers” in California, in conjunction with other local bar associations; and

• Convened a global meeting at the inaugural CLA Annual Meeting of Foreign Bar delegates from Malaysia, France, Japan, Mexico and Vietnam with whom the ILS has Friendship Agreements—an international bond recognized by the CLA leadership at the Annual Meeting.

We look forward to a great year ahead and working with you to continue our collective momentum in helping the ILS better serve our members and community.

**Alexandra Darraby and Michael R. Newman**  
ILS Co-Chairs

To join the ILS and for additional information, please visit us at www.calawyers.org/international, on Facebook @CLAInternationalLaw or on Twitter @CLA_ILS. Your ideas are valued and your participation in our programs is invited.

**Would you like to promote your organization, products or services?**

Please consider placing an advertisement in the *Journal*. With an extensive readership of legal practitioners in California, the U.S. as a whole as well as abroad, the *Journal* provides the perfect opportunity for promotion.

Please contact us for information about advertising opportunities and rates at ils@calawyers.org.
The International Law Section was founded in 1987 to serve California lawyers handling international legal matters in a wide variety of areas, including corporate and business transactions, immigration, litigation and arbitration, tax, regulatory and trade matters, bankruptcy, intellectual property and family law.

The Section organizes programs and events around the state, as well as publishes and distributes two key publications: The California International Law Journal, a collection of practical articles on various aspects of international practice, and an online newsletter, The California International Law Newsletter.

The International Law Section also presents MCLE-accredited programs throughout the year, regularly attracting attorneys and academicians for a weekday or weekend of discussions about current public and private international law topics.

Membership is open to California lawyers as well as to attorneys and other interested professionals and students worldwide. To join please go to www.calawyers.org/Join-Us. For additional information, please visit us at www.calawyers.org/international, on Facebook @CLAInternationalLaw, or on Twitter @CLA_ILS.
The International Law Section welcomed five foreign delegations to the first Annual Meeting of the California Lawyers Association (CLA) in September 2018. Attorneys from France, Japan, Malaysia, Mexico and Vietnam traveled to San Diego to attend CLA Meeting programs, share best practices and network with their California colleagues.

The ILS had long-standing relationships with many foreign bars under the State Bar of California, and those relationships transferred with the ILS to the new CLA during the reorganization this year. The first Annual Meeting of the CLA provided an opportunity for the ILS to formally renew several of those relationships and to establish new relationships through signing updated Friendship Agreements between the ILS/CLA and foreign partners.

Representatives from the Marseille Bar, the Malaysian Bar, the Osaka Bar, Asociación Nacional de Abogados de Empresa, Mexico (ANADE) and the Vietnam Lawyers Commercial Arbitration Centre made the trip to San Diego.

The foreign attorneys were welcomed to San Diego by ILS Co-Chairs, Alexandra Darraby and Michael Newman, at a reception before the Annual Meeting began, generously sponsored by: Seltzer Caplan McMahon Vitek; Maldanado Myers LLP; Sempra Energy; and Franco Serafini.

Many of the foreign visitors enjoyed a cruise on San Diego Bay with members of the ILS and all were welcomed and recognized at the Warren M. Christopher International Lawyer of the Year Award ceremony and dinner that followed. Leaders of the foreign delegations also attended and made presentations about their respective Bars at the ILS Executive Committee meeting, where the ILS Co-Chairs presented them with certificates of appreciation and gifts were exchanged.

This is the third year that the ILS has received representatives from Vietnam. The Vietnam Lawyers Association sent a delegation to Los Angeles in 2016 and another delegation attended the annual conference of the State Bar of California in 2017. This year’s delegates represented both the Vietnam Lawyers Commercial Arbitration Centre and the Ho Chi Minh City Commercial Arbitration Association. A visit by ILS members to Vietnam is proposed.

The Malaysian Bar, making its first visit to the U.S., took the opportunity to sign its first American Friendship Agreement with the ILS. That relationship was cultivated through the efforts of ILS Co-Chair Alexandra Darraby and Executive Committee Secretary Tiffany Heah.

The relationship with the Marseille Bar is also relatively new. ILS Co-Chairs Michael Newman and Alexandra Darraby were invited to present programs at a conference organized by the Marseille Bar in June. The relationship blossomed from that exchange and resulted in the visit to San Diego of a large delegation from France, following the signing of a new Friendship Agreement in June 2018 with the Marseille Bar.

ANADE and Osaka represent two of the ILS’s longest relationships. ANADE is the premier association of legal professionals in Mexico. The relationship was originally developed by previous ILS Chair, Enrique Hernandez, and is nurtured by Executive Committee members Agustin Ceballos and Lizbeth Flores.

Osaka is one of two relationships that the ILS has with Japanese bars. The other long-standing relationship is with the Daiichi-Tokyo Bar. The ILS has had numerous exchanges with the two Japanese Bars through the efforts of former ILS Chair, Harumi Hata, along with a number of other ILS members who have

Richard Bainter
Co-Chair, ILS Foreign Relations Committee

Year Award ceremony and dinner that followed. Leaders of the foreign delegations also attended and made presentations about their respective Bars at the ILS Executive Committee meeting, where the ILS Co-Chairs presented them with certificates of appreciation and gifts were exchanged.
professional ties to Japan, including ILS Co-Chair Michael Newman.

Under the new CLA structure and the leadership of the ILS Co-Chairs, the Executive Committee seeks to develop further agreements with foreign bars or lawyers associations that meet new criteria developed by the Foreign Relations Committee and approved by CLA. Equally important, the Executive Committee has placed an emphasis on implementing its Friendship Agreements with foreign bars to create meaningful interaction between California lawyers and their foreign counterparts. The visits by five foreign delegations to the 2018 annual conference is only one example of those efforts. ILS members can expect more opportunities for educational exchanges and cross-border cooperation in the future.

We welcome the participation of all ILS members in fostering our relationships with foreign bars or lawyers associations. If you have connections with any such organizations that may be interested in Friendship Agreements, or would like to assist with programming, please contact the ILS Foreign Relations Committee Co-Chairs Richard Bainter or Joshua Surowitz, at ils@calawyers.org.

From September 13 through September 16, 2018, the International Law Section actively participated in the First Annual Meeting of the California Lawyers Association in San Diego, hosting a mini-United Nations by inviting delegations of foreign bar associations from France, Japan, Malaysia, Mexico and Vietnam for the inaugural CLA Annual Meeting. For many delegates this was a first trip to the U.S.

The ILS has been honored by the CLA as the official Section designated to represent the CLA in forging and making Friendship Agreements with foreign bar associations around the globe. During the Meeting, the ILS and its foreign delegates were recognized and introduced by Heather Rosing, President of CLA.

In a special ceremony, the ILS and the delegation leaders of each foreign bar signed formal Friendship Agreements on behalf of the CLA. The ILS also invited the visiting foreign bar delegations to make presentations at its Executive Committee meeting, which resulted in plans to hold joint programming and exchange visits going forward for Section members.

A harbor cruise of San Diego Bay was hosted by ILS members for the five delegations, and throughout the Meeting representatives planned events for building relationships among the foreign bars.

On Friday evening, the ILS presented its Eighth Annual Warren M. Christopher International Lawyer of the Year Award. This prestigious award is intended to honor California legal practitioners who render extraordinary service to our profession in the field of international law.

Finally, the ILS presented four programs for CLE credit at the Meeting, covering many international law topics: Leonardo Da Vinci and the Cross-Border Sale of Personal Property in an Era of Cybercrime and Terrorism; Coming to the USA: Tax & Visa Planning; and The Nuts & Bolts of International Arbitration and From Aerospace to Art—A-Z: How to Plan for Successful International Careers in the Arts & Global Trade. The last program was specifically designed in partnership with the California Young Lawyers Association as part of a jointly sponsored International Career Program.

2018 CLA ANNUAL MEETING REPORT

* Brian Arbetter is a former Chair of the International Law Section and of the State Bar of California Council of State Bar Sections. He currently serves as the ILS Representative on the CLA Board of Directors. He is a partner with the global law firm Norton Rose Fulbright and focuses on domestic and global labor and employment law.
The International Law Section is pleased to honor Mitsuru Claire Chino, the recipient of the ILS’s Eighth Annual Warren M. Christopher International Lawyer of the Year Award.

This prestigious Award, presented annually by the ILS, is intended to honor California legal practitioners who render extraordinary service to our profession in the field of international law. The Award is named after its first recipient, Warren M. Christopher, who had a long and distinguished career both as a lawyer and statesman; among his many accomplishments as the 63rd Secretary of State, Mr. Christopher brokered the Bosnian Peace Agreement during President Bill Clinton’s first term in office.

The recipient of this year’s Award, Mitsuru Claire Chino, is the President & CEO of ITOCHU International Inc. and Managing Executive Officer of ITOCHU Corporation, a Fortune Global 500 company, headquartered in Japan, with over 40,000 employees worldwide. In 2013, she became the first female executive officer of any major trading company in Japan. She has also been active in promoting women’s interests in corporate Japan and was instrumental in initiating a diversity program within ITOCHU. Prior to joining ITOCHU, she was a partner of an international law firm. Claire has received numerous awards and recognitions throughout her career, including from the World Economic Forum (Young Global Leader), Yale University (Yale World Fellow), Asia Society (Asia 21) and the U.S. Japan Leadership Program. She has also been recognized in the in-house community as a “Top 25 In-House Counsel in Asia” (Asia Legal Business), “Asia Pacific’s Innovative Lawyer” (Financial Times) and “FT Global General Counsel 30 (Financial Times). Claire is a graduate of Smith College (B.A. cum laude) and Cornell Law School (J.D.), where she serves on the advisory board, and has taught as a Distinguished Practitioner in Residence.

In presenting the Award, ILS Co-Chair Alexandra Darraby emphasized that “international law is the bellwether of the global community in which all of us reside and work,” and that “the international lawyer, the good international lawyer, the effective international lawyer has to have certain attributes to make her or his role successful in this environment, including:

- open
- accepting
- curious
- interested
- interactive
- ethical
- an advocate of rule of law and mutual cooperation
- respectful of human dignity.”

The Warren M. Christopher Award is intended to recognize these qualities, in addition to each recipient’s extraordinary achievements.
Please join us for our next ILS Webinar

BIAS IN THE WORKPLACE

January 23, 2019
Time TBA
MCLE Credit Available

This webinar is a collaboration between the ILS and the Marseille Bar, which signed a Friendship Agreement with ILS.

On January 23, 2019, ILS will join the Marseille Bar in offering the first French-American CLE webinar on Bias in the Workplace. Moderator Jeffrey Daar of Daar & Newman will be joined by Alexandra Darraby of The Art Law Firm and ILS Co-Chair, as well as Madame Marie-Adélaïde BOIRON, Member of the Bar Council of Marseille and principal of Cabinet Boiron as well as the Delegation Leader of the Marseille Bar to the 2018 CLA Annual Meeting.

This is an opportunity to complete your MCLE requirements and learn about navigating fairness, propriety and equality in the legal work space and professional workplace in California and France.

The time for this webinar will be updated on our website, www.calawyers.org/international.

Upcoming webinars will also be listed on our website on an ongoing basis. For additional information about ILS webinars, and to view past webinars for MCLE credit, please visit https://cla.inreachce.com/ and click on the link for International Law.
The most important change in international legal affairs in 2018 for California lawyers and their clients was the legislature unanimously passing and Governor Brown signing Senate Bill 766 (SB 766), sponsored by Senator Bill Monning (D. Monterey). SB 766, signed by Governor Brown on July 18, 2018, effective as of January 1, 2019, permits a non-California lawyer qualified as a lawyer in another state or country to represent parties in international arbitrations in California. As international contracts, whether for financing, trade, joint ventures or suppliers, ordinarily include an international arbitration clause, SB 766 will have widespread effect.

It will not only bring more international arbitrations to California. It quite separately will provide additional leverage to California companies negotiating all international contracts.

I. INTERNATIONAL ARBITRATION IN CALIFORNIA PRE-2018

Despite being the fifth largest economy in the world, California has for decades been a backwater for international commercial arbitration. The problem began when the California Supreme Court decided Birbrower, Montalbano, Condon & Frank v. Superior Court, 7 Cal. 4th 119 (1998), which effectively held representing parties in international arbitration in California was considered unauthorized practice of law, and a non-California lawyer could not practice or collect fees for work on international arbitration in California. Since California Business and Professions Code section 6126 states penalties for unauthorized practice of law in California may include a fine of up to one thousand dollars and one year in county jail, lawyers around the world were told if they went to California to handle an international arbitration, under a technical reading of the California statutes, they could go to jail. Non-U.S. lawyers negotiating with California businesses with respect to contracts that contained international arbitration clauses were simply unwilling to agree to California as a venue for arbitration, since they would not be able to appear and represent their clients in the arbitration and could be subject to severe penalties.

Before SB 766, if counsel for a California company during negotiations of an international contract suggested seating an international arbitration in California, the non-California counterpart could quickly say: “How do you expect me to agree to a procedure in California in which I am legally prohibited from appearing on behalf of my client?” There was no satisfactory answer. Now there is.

II. SB 766’S SIGNIFICANT CHANGES

SB 766 was designed to and did completely solve the problem of foreign lawyers appearing in arbitrations sited in California. Non-U.S. lawyers can no longer oppose arbitrations in California based on a lack of their ability to appear.

SB 766 is very straightforward on this point, and California lawyers should be familiar with the new law and be able to discuss it.

SB 766 is chaptered as California Code of Civil Procedure (CCP) sections 1297.185 et seq, and includes CCP section 1297.186(a), which provides that a non-California attorney who is admitted to practice in any state or foreign jurisdiction “may provide legal services in an international commercial arbitration or related conciliation, mediation or alternative dispute resolution proceeding, if any of the following conditions is satisfied:

1. The services are undertaken in association with an attorney who is admitted to practice in this state and who actively participates in the matter.

2. The services arise out of or are reasonably related to the attorney’s practice in a jurisdiction in which the attorney is admitted to practice.

3. The services are performed for a client who resides in or has an office in the jurisdiction in which the
attorney is admitted or otherwise authorized to practice.

(4) The services arise out of or are reasonably related to a matter that has a substantial connection to a jurisdiction in which the attorney is admitted or otherwise authorized to practice.

(5) The services arise out of a dispute governed primarily by international law or the law of a foreign or out-of-state jurisdiction.”

(emphasis added) These provisions are sufficiently broad that any attorney admitted to practice in a foreign jurisdiction should be able to appear in an international arbitration in California. California lawyers should have these provisions available during conversations with foreign counsel who may not be aware of the straightforward nature of SB 766.

III. IMPLICATIONS OF SB 766 IN NEGOTIATING ARBITRATION CLAUSES

SB 766 is especially useful for California-based companies. As a matter of cost and convenience it would be helpful for most California companies to have international arbitrations venued in California. Costly travel can be avoided, and their own counsel, familiar with their industry and company, could be here for the arbitration.

Even after SB 766’s clarification about their ability to appear, foreign counsel may still raise objections to basing arbitrations in California.

For example, foreign counsel may want to avoid the application of California law. There may be two stated reasons for this. First, consumer, employment and general domestic arbitration cases in California have imposed stringent rules on general arbitration in California, including arbitrator disclosure rules that do not apply to international arbitrations in California, which are governed solely by the California International Arbitration and Conciliation Act, CCP sections 1297.11 et seq. California counsel should have copies of the California International Arbitration and Conciliation Act, which now includes all the provisions of SB 766’s CCP section 1297.186(a), to send to foreign counsel to answer clearly any confusion they may have about its defined scope and effect.

Second, foreign counsel may object to the use of California substantive law. The parties to an arbitration agreement can choose which substantive law applies as a matter of contract. So, for example, the parties may agree that English, or New York or other substantive law governs the arbitration. Foreign counsel should also be reminded that California international arbitrations will be governed and subject to the same rules as any other jurisdiction under the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, known as the New York Convention.

Additionally, despite California having a group of the most experienced and respected arbitrators in the world, foreign lawyers may want one or more arbitrators to come from outside California. But there is no restriction on having foreign arbitrators come to California, so there is no reason to choose the venue for that reason.

As shown above, what SB 766 does is open negotiations as to the place of the arbitration. California companies and counsel may ultimately decide to go elsewhere, but if that happens there will have been leverage in the negotiations to help achieve other goals.

IV. IMPLICATIONS FOR THE STATE OF CALIFORNIA

Because of SB 766, international arbitration should now be able to grow as fast in California as it has in other parts of the world. California is home to the technology and entertainment industries, two of the essential drivers of global growth. The economic development potential for the state of California is enormous. Indeed, what drove approval of SB 766 in the committee hearing in the California legislature was exactly this point.

With the passage of SB 766, lawyers and arbitral institutions around the world will need to recognize California is now open for international arbitration business, and the excuse foreign counsel, companies and arbitral institutions once had for avoiding California is now gone. Pacific Rim international arbitrations should come here instead of to venues in Asia. NAFTA, Central and South American arbitrations should come here as well as to Miami.

To assist in bringing in the new age of international arbitration in California, a group of counsel and neutrals with experience in issues of international arbitration formed, in July of this year, the California International Arbitration Council (CIAC), a new non-profit, to promote California international arbitration. The Council (www.ciac.us) will reach out internationally, work with state and local governments and plan programs to help all lawyers and businesses in California benefit from the growth of international arbitration.
The influence SB 766 will likely have in increasing international arbitration in California will also aid the growth of other alternative means of dispute resolution in this state. California is home to an experienced and sophisticated mediation culture. The word for mediation in international dispute resolution is conciliation. It is not used internationally as much as it should be, although that may be changing. The United Nations Commission on International Trade Law (UNCITRAL), is drafting a settlement convention for international commercial settlements to provide for their enforcement in the same way the New York Convention enforces arbitration awards.

There is a real potential for California-based mediation and other dispute resolution practice to not only grow but to have influence worldwide.

We are beginning a new age in California for international dispute resolution. It is important that international law practitioners are aware of these changes. It is equally important we carry the message to our colleagues, so they are fully aware of the potential in any transaction or dispute with international implications.

* Howard B. Miller is a JAMS Mediator and Arbitrator, a past president of the State Bar of California and a Founder and Co-Chair of the California International Arbitration Council. He can be reached at hmiller@jamsadr.com.

---

**Become a Sponsor!**

The International Law Section is accepting additional annual corporate sponsors, as well as event/program specific sponsors.

Please join the International Law Section as a valued sponsor and be recognized.

If you are interested in becoming a sponsor of the International Law Section, please contact us for details of the annual corporate sponsorship and other sponsorship opportunities at ils@calawyers.org
A U.S. District Court decision in California has strengthened the legal foundation for the Securities and Exchange Commission (SEC) in its initiative to enforce federal securities laws in the marketing of investment opportunities under the EB-5 immigrant investor visa program, and underscored the risk of ignoring those laws. In the closely watched case SEC v. Feng, the court issued two noteworthy holdings:

- EB-5 investments are “securities” under the federal securities laws and subject to regulation under those laws.
- An attorney who acts as a broker for a client’s investment in an EB-5 investment opportunity must register with the SEC as a broker-dealer.

In reaching its conclusions the Feng court also affirmed, in the EB-5 context, that information about the payment of referral fees or commissions to intermediaries is material to investors as a matter of law, and that an immigration attorney who participates in an offering and omits disclosure of his receipt of commissions is liable under the anti-fraud provisions of the securities laws. Issuers and others who omit this information “in connection with the offer or sale of a security” would face similar statutory liability.

The defendants, Hui Feng and his law firm, are immigration attorneys based in Flushing, New York. Over several years Mr. Feng and the firm recommended EB-5 investment opportunities to clients seeking U.S. residency. Mr. Feng and the firm collected sales commissions and referral fees from the promoters of these offerings, often through offshore agents that appeared unrelated to Mr. Feng but that he owned and controlled. Approximately 100 clients purchased EB-5 investments from approximately five regional center sponsors through these recommendations. The majority of Mr. Feng’s clients did not know that he or his affiliates received commissions on the clients’ investments.

The court determined that it had received sufficient uncontested evidence to rule for the SEC by summary judgment on all points of the agency’s civil enforcement suit—that is, without the need for a trial. The court found Feng liable for unregistered broker-dealer activity and for violating the anti-fraud statutes of both major federal securities laws by concealing his referral fees from clients and from regional centers sponsoring projects that offered the investments. The ruling requires Feng and his firm to disgorge approximately $1.8 million in unlawful commissions (including interest), pay nearly $1 million in civil penalties and permanently enjoins them from further violations of the federal securities laws.

The EB-5 Immigrant Investor Program was created by Congress in 1992 to encourage foreign investment in U.S. job-creating activities. Investors who invest $500,000 or $1,000,000 (depending on location) in an eligible project may apply to the United States Citizenship and Immigration Services (USCIS) to receive conditional U.S. residency for themselves and their immediate family. If the project successfully creates 10 jobs for each investor, the investors may apply to USCIS to remove their conditions to residency and receive permanent, unconditional residency. “Regional centers” are entities authorized by USCIS to sponsor and promote EB-5 investments in projects within a specified territory. Most, but not all, EB-5 projects affiliate with an authorized regional center because regional center sponsored projects can prove job creation based on economic modeling rather than strictly based on payroll.

The Feng case is one of several similar civil enforcement actions involving EB-5 investments that the SEC initiated in 2015. Other than Feng and his firm, all defendants in those actions settled with the SEC prior to any court proceedings. Feng has argued that under the well-established “Howey test,” EB-5
Investments are not “securities” within the definition of the federal securities laws because the investors seek immigration benefits rather than profit. He has argued that the SEC’s enforcement actions against immigration attorneys for unregistered broker-dealer activities in EB-5 offerings represent the agency’s unwarranted over-reach beyond its jurisdiction to interfere in the attorney-client relationship.¹⁶

Feng characterized the issue of whether EB-5 investments are securities as an “issue of first impression,” that is, a novel issue for the court, for which no binding legal precedent exists.⁷ However, the court did not treat the question as an issue of first impression and cited binding Ninth Circuit and U.S. Supreme Court precedents for its holdings. In finding that EB-5 investments satisfy the Howey test’s requirement of “an expectation of profit from the efforts of others,” the court relied on the following observations:

• Even when investors primarily invest for reasons in addition to profit, they may have sufficient “expectations of profit” to find that the investments are securities.⁸ In other words, EB-5 investors could be investing to gain U.S. residency and investing for financial reasons.

• The EB-5 program regulations themselves state that the investors’ capital must be “put at risk for the purpose of generating a return on the capital placed at risk.”⁹

• While Feng argued that, subjectively, EB-5 investors did not expect a return on investment, the law instead focuses on whether the objective terms of the offering created an expectation of profit, and the terms of the EB-5 offerings in question did discuss the potential for profit.¹⁰

• Even if the investors must pay an administrative fee that is greater than potential profits, the court should not “conflated” fees and the purchase price in assessing whether the proceeds of an offering were intended to be profitable.¹¹

In arguing against treatment of EB-5 investments as securities, the defendants relied on United Housing Foundation, Inc. v. Forman, in which the Supreme Court suggested that for an instrument to be deemed a security, the investor must be “solely attracted by the prospects of a return.”¹² The Feng court found that Forman does not require profit to be an investor’s sole purpose, citing cases in the Ninth and Second Circuits, decided after Forman, in which investments promoted primarily for tax benefits were nonetheless deemed securities under the Howey test.¹³

After determining EB-5 investments are securities, the court found no basis to exempt immigration attorneys from the SEC’s regulation of brokers and dealers. The court looked to eight factors typically used to determine if an individual must register as a broker-dealer—the most important of which is the receipt of transaction-based fees such as commissions—and found that the defendants satisfied seven of the eight factors.¹⁴ It found that the defendants therefore acted as broker-dealers and should have registered under the Securities Exchange Act of 1934 as amended (Exchange Act).

The court then examined the defendants’ failure to tell clients that they received referral fees for placing their investments, and stated that as a matter of law, withholding such information is a “material omission” under the antifraud provisions of the Securities Act of 1933, as amended (Securities Act).¹⁵ Usually, a finder of fact at a trial must determine whether omitted information was material to investors. However, the court was bound by precedents establishing that reasonable minds cannot differ on the materiality of an advisor’s financial motivation and its potential conflict of interest in recommending an investment.¹⁶

Beyond the mere omission of material information, the court found that in this specific case the defendants acted with “scienter”—an intent to deceive or defraud. The court pointed to the defendants’ admission that they “knowingly failed to disclose their receipt of commissions because they wanted to avoid having to negotiate with clients about rebating portions of the commissions.”¹⁷ Moreover, the court concluded that the defendants acted in furtherance of a “scheme to defraud.” In particular, Feng tried to make it appear that rebates to clients on his commissions were being paid not by him but by the regional center, and admitted in deposition that his purpose was to avoid further negotiations on rebates. Feng also led regional centers to believe they were paying commissions to an independent Chinese agent, when he actually owned and controlled the agent. The court concluded that Feng violated both Section 10(b) of the Exchange Act (under Rule 10b-5) and Section 17(a) of the Securities Act.¹⁸

As a necessary element to fraud liability under those statutes, the court had to determine that Feng made the omission “in connection with an offer or sale of securities.” Feng argued that because his payments were triggered by immigration action—USCIS acceptance of the investor’s application for residency—they were not made in connection with a securities transaction. The court found this distinction to be a mere formality: Feng’s client invested in securities in reliance on his recommendations,
The SEC did not assert that any of the investments that the defendants recommended involved fraud, or that the investor-clients lost any invested funds because of the defendants’ actions. Rather, the court found the commissions themselves to have been fraudulently obtained, resulting in civil penalties in addition to disgorgement.

While Feng may have misled them as to the ultimate recipient of the commissions, the regional centers that offered the EB-5 investments were certainly aware that commissions were paid. The Feng pleadings and decisions do not say whether the regional centers disclosed this information to investors, but under the court’s reasoning they too could have liability for omitting material information in connection with a securities transaction.

**PRACTICAL LESSONS**

While some may argue to the contrary, both USCIS and the SEC treat EB-5 investment opportunities as securities subject to the federal securities laws. Proposed legislation to reform the EB-5 program would likely remove any doubt that EB-5 investments are covered by federal securities laws by expressly requiring compliance. However, it is uncertain when or if Congress will adopt EB-5 reform legislation. In the meantime, the SEC’s ability to apply federal securities laws to EB-5 investments rests on the principles laid down in decades of case law interpreting the scope of those laws.

As the decision of a District Court in the Ninth Circuit, the Feng case is not binding on other federal courts, and Feng has filed an appeal in the Ninth Circuit. The court itself noted that part of its holding relied on precedents in the Ninth and Second Circuits, leaving open the possibility that higher courts or courts in other circuits—and ultimately the Supreme Court—might disagree. Nevertheless, even die-hard adherents to the view that the SEC has no authority over EB-5 offerings should by now realize that acting on that belief is too risky. Those willing to roll the dice based on past industry practices should not expect lenient treatment in a future enforcement action based on a good faith belief that securities laws did not apply to EB-5, because such a belief is no longer plausible.

Key takeaways from the case include the following:

- **Treat EB-5 offerings as securities offerings.** Among other things, this means the offering must be eligible for an exemption from registration under the Securities Act (unless registered with the SEC), and the issuer must disclose all material information to the investor. Well-advised EB-5 issuers have long been following this course.

- **Compensated EB-5 intermediaries in the U.S. must register.** If EB-5 investments are securities, it follows that anyone in the business of facilitating the sales of EB-5 investments could be a broker-dealer, and someone who gets success fees for such activities in the U.S. likely must register. This would include attorneys introducing clients to issuers who pay referral fees to the attorney, and regional centers that advertise for investors and introduce them to sponsored projects for fees. Broker-dealer registration may be expensive and onerous, but brokering without registration is illegal. Regional centers and others in the U.S. who plan to be compensated for marketing EB-5 offerings have increasingly sought to register as broker-dealers or to affiliate with registered broker-dealers.

- **Offshore agents should avoid establishing U.S. branches or affiliates unless they are prepared to register in the U.S.** Offshore agents that are not affiliated with U.S. parties and do no brokering business in the U.S. are likely exempt from U.S. registration requirements as “foreign broker-dealers.” However, any arrangement by which a foreign entity receives compensation for EB-5 brokering activities conducted in the U.S. may be viewed as a fraudulent scheme to avoid regulation. This includes not just selling to U.S. investors, but assisting a U.S. issuer in selling securities to offshore investors, which also involves activities that require broker-dealer registration. Moreover, if a foreign broker opens a U.S. branch, it exposes the entire global operation to U.S. broker-dealer regulation, and even establishing a U.S. corporate affiliate of a foreign broker-dealer requires the U.S. affiliate to register, even if all sales activities are directed outside the U.S.

- **Compensation to intermediaries must be disclosed to investors.** This applies to issuers as well as U.S.-based intermediaries. The Feng court’s statement that compensation of intermediaries is intrinsically material as a matter of law is not new, and follows established precedents. Beyond argument, a reasonable investor would want to know who is compensated and how much they are compensated for recommending a specific investment. Offshore EB-5 placement agents often pressure U.S. issuers to omit disclosure of commissions from their offering documents; issuers must be prepared to insist that they will comply with U.S. securities laws.
Attorneys may generally advise clients about EB-5 investments. The Feng defendants argued that SEC authority over EB-5 investments would prevent attorneys from acting as a “first line of defense” against fraud by warning them away from bad projects.27 However, as noted by the Feng court, an attorney who advises a client on the advisability of an investment will not be required to register under the Investment Advisors Act of 1940 if “the performance of such services [is] solely incidental to the practice of [their] profession.”28 As a result, an attorney who receives no commission or referral fee (and otherwise avoids being a broker), and who is acting within the overall scope of immigration legal advice, should be able to advise a client on the advisability of making an EB-5 investment without fear of triggering an SEC registration requirement.

SEC enforcement action may be only the beginning of legal travails for the defendants in Feng and for other lawyers who conceal commissions received as unregistered brokers. If investors experience losses in their EB-5 investments, they may seek recovery from the lawyer in a private securities action based on principles of fraud.29 Similarly, lawyers who receive no commission or referral fee (and otherwise avoid being a broker) and who are acting within the overall scope of immigration legal advice, should be able to advise on the advisability of making an EB-5 investment without fear of triggering an SEC registration requirement.

Legislation that would definitively show Congress’s intent to regulate EB-5 investments under the federal securities laws has been proposed but remains on the far horizon. Nevertheless, the apparent ease with which the Feng court reached its conclusions under existing law should demonstrate that litigating with the SEC over its authority in EB-5 can be a highly unproductive investment of time and money. And even a victory would likely be rendered moot when Congress ultimately adopts EB-5 reform legislation requiring federal securities law compliance.

Those who choose to fight a similar SEC enforcement action on principle rather than settling should also consider that the discovery process may reveal messy facts. In this case, the defendants’ admission in depositions that they concealed their referral fees from clients to avoid negotiating a rebate on fees cannot have helped their argument that their duties as attorneys adequately protected their clients’ interests as investors. Similarly, the defendants’ efforts to conceal their ownership of a Chinese company receiving commissions, which the SEC brought to light and the court labeled “a scheme to defraud,” would not have helped persuade a court that the SEC’s interest in the case was an unwarranted excursion beyond the agency’s lawful mission.

For immigration attorneys involved in EB-5, the message is clear: be careful who pays you and what they pay you for, or you may get a call from the SEC.

ENDNOTES

2 Id. at 15 (citing SEC v. Phan, 500 F.3d 895, 903 (9th Cir. 2007); TSC Indus. v. Northway, Inc., 426 U.S. 438, 450 (1976)).
5 Hui Feng’s Answer to Complaint, Case No. 2:15 cv-09420 – CBM (SSx) (“Defendants’ Answer”), at 7, 20.
6 Defendants’ Answer, at 1.
8 Feng, No. 15-cv-9420-CBM-SS, 2017 U.S. Dist. LEXIS 103592, at *2 (citing 8 C.F.R. §204.6(j)(2)).
9 Id. at *9 (citing Howey, 328 U.S. at 298-99; S.E.C. v. C.M. Joiner Leasing Corp., 320 U.S. 344, 352-53 (1943)).
10 Id. at 10 (citing S.E.C. v. Liu, 2016 U.S. Dist. LEXIS 181536, at *12).
13 As set forth in S.E.C. v. Hansen, 1984 WL 2413, at *10 (S.D.N.Y. Apr. 6, 1984), the court considers whether the individual:
14 (1) is an employee of the issuer of the security;
15 (2) received transaction-based income such as commissions rather than a salary;
16 (3) sells or sold securities from other issuers;
17 (4) was involved in negotiations between issuers and investors;
18 (5) advertised for clients;
19 (6) gave advice or made valuations regarding the investment;
20 (7) was an active finder of investors; and
21 (8) regularly participates in securities transactions.
22 The court found that all factors except the first were satisfied.
23 Among immigration attorneys, Feng may be unusual in the number of factors he personally satisfied. For example, the court
24 * Charles Kaufman practices corporate, securities and business transactional law in Los Angeles. He received his J.D. from UCLA School of Law and a B.A. in English from UCLA. He is a member of the State Bar of California.
cited evidence that Feng had previously traded securities and operated a hedge fund.

16 Id.
22 See supra n.1. The appellant’s opening brief reiterates the argument, under Forman, that an investor must be solely motivated by the prospect of a return on investment for securities laws to apply and, among other things, argues that the definition of “broker” under Section 15(a) of the Securities Exchange Act is “unconstitutionally vague.” (Defendants’ and Appellants’ Opening Brief).
23 Rule 15a-6, Exchange Act.
24 Counseling issuers in the structuring of securities transactions is generally considered brokering, especially if commissions are received. Andrew Tuch, The Self-Regulation of Investment Bankers, The Geo. Wash. L. Rev. 120 (Dec. 2014).
26 In the EB-5 industry, fair disclosure of compensation to intermediaries has only recently become commonplace. While the more seasoned EB-5 placement agents in countries like China generally raise no objection, EB-5 issuers have recently reported to the author that placement agents in less established territories like Vietnam, India and Pakistan have demanded that issuers conceal commission information from investors.
29 The SEC’s legal ethics expert submitted a declaration to the Feng court opining that Feng had failed to satisfy ethical disclosure requirements. Feng, No. 15-cv-9420-CBM-SS, 2017 U.S. Dist. LEXIS 103592, at *16.

Do you have an article you would like published? Or maybe an idea for one?

THE CALIFORNIA INTERNATIONAL LAW JOURNAL welcomes and encourages the submission of articles from its readers and others!

For more information please contact:
Catherine L. Carlisle and/or Hera U. Smith at ils@calawyers.org.
I. INTRODUCTION

Cyber-based attacks have distinct advantages over physical attacks: they can be conducted remotely, anonymously and cheaply. They do not require significant investment in weapons, explosives or personnel. And yet, their effects can be both widespread and profound. As of 2000, Interpol estimated that there were as many as 30,000 websites that provided automated hacking tools and software downloads. As of 2002, 19 million individuals had the knowledge necessary to launch cyber attacks. And as of 2008, the Defense Department estimated more than three million attacks occur annually. Worldwide aggregate damage from these attacks is now measured in billions of U.S. dollars annually.

Little specialized equipment is needed: the basic attack tools consist of a laptop, modem, telephone and software used daily by countless professionals. Recently, the attacks have shifted from espionage to destruction; nations are actively testing how far they can go before the state will respond. For example, following reports of infiltration by foreign spies, the U.S. government did little more than admit that the nation’s power grid is vulnerable to cyber attack. Alarmingly, the software left behind in these attacks reportedly had the capability of shutting down the country’s electric grid. Former CIA operative, Robert Baer, stated that these types of attacks are not uncommon:

[Other countries’] foreign intelligence service has been probing our computers, our defense computers, our defense contractors, our power grids, our telephone system … I just came from a speech at the national defense university and they were hit by the Chinese trying to get into their systems. They are testing and have gotten in portals. It’s a serious threat.

Cyber attacks that are reasonably expected to cause injury or death to persons, or damage or destruction to objects, are generally illegal under international law. However, such an attack may be permissible if: (1) the attack is undertaken by the armed forces of the state; (2) the attack effectively distinguishes between military and civilian personnel and objects; (3) the attack respects the jus in bello principles of necessity and proportionality; and (4) the attack occurs during an armed conflict. Part II will examine the question of attribution for cyber attacks, while Part III will emphasize the controlling factors for the legality of cyber attacks in the context of an armed conflict. Finally, Part IV argues that cyber attacks attributable to the state that are reasonably expected to cause injury or death to persons or damage or destruction to objects are impermissible under international law outside of a recognized armed conflict, with perhaps an exception for self-defense under Article 51 of the Charter of the United Nations.

II. ATTRIBUTION OF CYBER ATTACKS

A. Definition of a Cyber Attack

The first question to address is what, exactly, constitutes a cyber attack? The Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism defines cyber attacks as: “[The] intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm.” A broader definition of cyber attacks may be found in the U.S. Department of Defense’s Dictionary of Military Terms, which defines a “computer network attack” as “[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” By comparison, the Tallinn Manual on the International Law Applicable to Cyber Warfare contains a narrow definition: it defines a cyber attack as “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”
The characterization under the Tallinn Manual—limiting the scope to any resulting “injury or death” and “destruction to objects,” while excluding purely economic harm—is the most applicable to customary international law on the use of force. Although all of the incidents described by the Stanford Draft International Convention and the Dictionary of Military Terms compromise the security of a computer network, mere cyberespionage or cyber-exploitation does not constitute a cyber-attack for the purposes of this analysis.

After the act is defined, the next problem is whether the cyber attack is attributable to the state. There are two possible scenarios in which a cyber attack is attributable to a state: (1) when a state permissively allows its territory to be used to carry out the attack (such as when a state offers safe haven to a terrorist organization that conducts a cyber attack); or (2) when a state overtly or implicitly directs the acting party engaging in the particular conduct (such as when a state orders its armed forces to undertake a cyber attack).

### B. Territorial Attribution of a Cyber Attack

It is well established in international law that the “effects principle” permits the extraterritorial regulation of activities that impact a state’s territory. For example, the Third Restatement of Foreign Relations Law states that international law recognizes that a nation may provide rules with respect to “conduct outside its territory that has or is intended to have substantial effect within its territory.” Although this type of territorial integrity is a fundamental principle of international law and relations, it is difficult to apply to “commons” such as cyberspace. Hence, although a state may establish domestic cyber law, imposing it is another matter.

And although the existence and enforcement of domestic law criminalizing cyber attacks is one way to lessen the liability of a state for attacks independently perpetrated by private actors, based on the effects principle, even those acts not sanctioned by the state’s domestic law may still be considered attributable to that state. If the state knew or should have known its territories were being used for acts against other states, it may be in violation of the law.

The attributable conduct can consist of both actions or omissions: in the Corfu Channel case, for example, the International Court of Justice (ICJ) held that it was a sufficient basis for Albanian responsibility that it knew, or must have known, of the presence of mines in its territorial waters and did nothing to warn other states of their presence. Similarly, the 1986 Libya precedent demonstrates that states that unwittingly, or permissively, allow their territory to be used to carry out attacks are guilty of committing an act of aggression themselves. In that case, the U.S. intercepted messages between Tripoli and Libyan agents in Europe in which the Libyan leader, Colonel Gaddafi, allegedly ordered an attack in West Berlin that killed two U.S. servicemen. In the trial that followed, the Berlin court held that Libya was to a large extent responsible for the attack, as the attack had been planned and carried out by members of the Libyan secret service in the Libyan Embassy in East Berlin.

Yet the analysis cannot end by simply determining the point of origin. Unlike Corfu Channel or the Libyan precedent, the fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence in and of itself to attribute the operation to that state; often, attacks are routed through multiple nations before the intended target is reached. The transnational realities of cyberspace are such that satisfactory territorial attribution depends largely on the actual knowledge of the state.

A good example is the United States Diplomatic and Consular Staff in Tehran: in that case, fifty-two U.S. diplomats and citizens were held hostage for 444 days after a group of Iranian students belonging to the Muslim Student Followers of the Imam’s Line, who were supporting the Iranian Revolution, took over the U.S. Embassy in Tehran. There, the ICJ held that the Islamic Republic of Iran was responsible due to the “inaction” of its authorities, which “failed to take appropriate steps” in circumstances where such steps were evidently called for. The court concluded that the actions of a state’s citizens could be attributed to the government if the citizens “acted on behalf on [sic] the State, having been charged by some competent organ of the Iranian State to carry out a specific operation.”

While the court did not obtain enough evidence to attribute the actions of the citizens to the government in that specific instance, the ICJ did determine that the Iranian government was nonetheless responsible on the grounds that it was aware of its obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff, and failed to comply with its obligations. In other words, if there is insufficient evidence to find attribution outright, then governmental awareness may be sufficient to establish a violation of law. Thus, in the context of a cyber attack, a state may be held in violation of international law by permissiveness established by its awareness of—and inaction towards—an illegal act or acts originating in its territory.
C. Organizational Attribution of a Cyber Attack

As to the second scenario, there are situations in which a state may have overtly or implicitly directed the party engaging in the disputed conduct. The simplest example, of course, would be if the armed forces of a state (as compared to unaffiliated citizens) acted under government command. In that case, attribution to the state for the cyber attack would be indisputable. However, even the acts of non-government parties—or even non-state parties—may still result in state liability for the attack. There may even be adequate evidence of state responsibility in situations where the conduct occurred entirely outside the state’s borders by actors of independent nationalities. In that situation, the analysis is, then, whether the state in question exercised adequate “territorial control” over the actors in question.

There are two standards in tension when determining adequate territorial control: the doctrine of effective control and the doctrine of operational control.29 The effective control doctrine, originating in the ICJ’s Nicaragua case, recognizes a country’s effective control over paramilitaries or other non-state actors only if the actors at issue act in “complete dependence” on the state.30 In contrast, the operational control doctrine, illustrated by the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the Tadic case, held that where a state has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control so that the group’s acts are attributable to the state.31

Therefore, a cyber attack could be attributable to a state if the state had either (1) “complete dependence” over those actors perpetrating the act under the Nicaragua standard; or (2) awareness that the cyber act was occurring or likely to occur, and failed to take appropriate remedial measures. Notably, despite conflicting precedents, the ICJ has consistently used the more restrictive Nicaragua standard in its jurisprudence.32 If there is no state nexus—that is, if the act was undertaken solely by private actors with no connection to the state whatsoever—then the cyber attack would be purely a matter of domestic law. After ascertaining responsibility, we next turn to the issue of whether cyber attacks would be permissible under international law during an armed conflict.

III. WARTIME CYBER ATTACKS

Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict, or international humanitarian law (IHL), if there is a nexus between the cyber attack and the armed conflict.33 Under IHL, a cyber attack may be permissible if: (1) the attack is undertaken by the armed forces of the state; (2) the attack effectively distinguishes between military and civilian personnel and objects; and (3) the attack respects the jus in bello principles of necessity and proportionality.

A. Permissible Participants in a Cyber Attack

In an armed conflict, the law contemplates only two categories of persons: civilians and combatants.34 Although all members of the armed forces of a party to the conflict are combatants, according to the Hague Conventions only members of a nation’s regular armed forces are entitled to use force against an enemy.35 Conversely, a combatant may be targeted solely based on his or her combatant status.36 They are legitimate military targets, and as such can be attacked until hostilities cease.37 However, combatants cannot conceal their allegiance; they must be recognizable as combatants while preparing for or during an attack:38

Under the principle of distinction, all involved in armed conflict must distinguish between … the combatants, on the one hand, and civilians on the other hand. Combatants must, therefore, distinguish themselves (i.e., allow their enemies to identify them, from all other persons, the civilians, who may not be attacked nor directly participate in hostilities).39

Under Protocol I, Article 44, soldiers who do not identify themselves as combatants by wearing a uniform or by carrying arms openly during or in preparation for the engagement would likely be stripped of their combatant privilege by a tribunal.40 The “combatant’s privilege” entitles an individual engaging in hostilities to protection from being criminally prosecuted for merely taking part.41 Combatants are allowed, within explicit guidelines, to use force and perform acts that would be considered criminal in a civilian context—such as murder, assault and damage to property—without being regarded as offenders.42

There are three primary limitations on the combatant’s privilege.43 First, the combatant must be acting on the state or group’s behalf.44 Second, combatants are not entitled to immunity for war crimes.45 Third, only combatants are entitled to claim the combatant’s privilege.46 Therefore, individuals not members of the armed forces—and those who fail to uphold the requirements of the privilege while perpetrating a cyber attack—would be considered in violation of Protocol I.

However, how do individuals properly identify themselves or openly carry arms in a medium such as cyberspace? A computer
is certainly not a weapon in the traditional sense, and uniforms mean nothing in the virtual world. In combat situations, distinctive signs may replace service uniforms—particularly in covert operations. They are often used to mark an item of the uniform—such as a beret, arm patch or lanyard. It is unclear whether such provisions would extend to cyber operations, though if so, likely the IP address of the military computer could serve as sufficient identification.

Unfortunately, the internet is the ideal platform for plausible deniability. States generally do not engage in cyber attacks openly, but rather tend to try to hide their responsibility through technical means and by perpetrating the attacks through non-state actors with ambiguous relationships to state agencies. For example, a cyber weapon reportedly designed by Israel and the U.S. was launched against Iran as early as 2008. The weapon targeted cascades and centrifuges at the Natanz uranium enrichment plant in Iran in an effort to set back Iran’s ability to produce a nuclear weapon. Cyber attacks such as this, not undertaken openly by a branch of the state’s armed forces, would constitute an illegal use of force—perhaps even rising to the level of an armed attack.

**B. The Principle of Distinction in a Cyber Attack**

As previously stated, computers are not the traditional weapons of an armed attack. Under international law, all new weapons, means and methods of warfare should be subject to rigorous and multidisciplinary review. This analysis includes humanitarian concerns, for example, as seen in the ICJ Advisory Opinion on nuclear weapons:

\[\text{The principles and rules of law applicable in armed conflict—at the heart of which is the overriding consideration of humanity—make the conduct of armed hostilities subject to a number of strict requirements. Thus, methods and means of warfare, which would preclude any distinction between civilian and military targets, or which would result in unnecessary suffering to combatants, are prohibited. In view of the unique characteristics of nuclear weapons, to which the Court has referred above, the use of such weapons in fact seems scarcely reconcilable with respect for such requirements.}\]

Similarly, cyber attacks that directly and intentionally result in non-combatant deaths and destruction of property breach modern prohibitions on the use of force. General Assembly Resolution 2444 (XXIII) affirms that a party’s right to injure the enemy is not unlimited, that attacks against civilian populations are prohibited and that the distinction between persons taking part in hostilities and members of the civilian population must be made at all times. General Assembly Resolution 2675 (XXV) reiterates the aforementioned, as well as further emphasizes that fundamental human rights continue to apply fully in situations of armed conflict, and that civilian populations, dwellings, installations, places or areas designated for the sole protection of or use by civilians should not be the object of military operations.

For instance, the apparent Israeli shellfire that knocked out the Gaza Strip’s only electrical power plant in 2014 worsened the humanitarian crisis for the territory’s 1.7 million people. Damaging or destroying a power plant, even if it also served a military purpose, would be an unlawful disproportionate attack under the laws of war, causing far greater civilian harm than military gain. The shutdown of the Gaza Power Plant drastically curtailed the pumping of water to households and the treatment of sewage. It also caused hospitals, already straining to handle the surge of war casualties, to increase their reliance on precarious generators. Finally, it affected the food supply by shutting off refrigerators and forced bakeries to reduce their bread production.

A pointed cyber attack could have similar effects, and be equally unlawful. The President’s Commission on Critical Infrastructure Protection (PCCIP), a group charged with assessing the U.S.’ vulnerability to computer attacks, has identified five critical infrastructures whose incapacity or destruction would cripple the nation’s civilian population: information and communications, physical distribution, energy, banking and finance and vital human services. This infrastructure, if the object of a cyber attack, would suffer the same harm as if the target of a more traditional weapon, such as an explosive. By giving rise to substantially the same kinds of harm as those found in accepted modes of warfare, certain cyber attacks could potentially be categorized as indiscriminate armed attacks if directly and intentionally resulting in non-combatant deaths and destruction of property.

**C. The Principles of Necessity and Proportionality in a Cyber Attack**

Furthermore, during an armed conflict, cyber attacks must be governed by the principles of necessity and proportionality. The law of war requires that parties distinguish between military and civilian personnel, objects and installations, and limit attacks to military objectives. Article 52.2 of Protocol I states that “military objectives are limited to objects that are effective contributions to military action and whose destruction offers a military advantage.” In other words, infrastructure that makes...
Military necessity is governed by several constraints: an attack or action must be intended to help in the military defeat of the enemy, it must be an attack on a military objective and the harm caused to civilians or civilian property must be proportional and not excessive in relation to the concrete and direct military advantage anticipated. The principle of humanity itself dictates of public conscience.

As earlier acknowledged under the principle of distinction, a cyber attack that fails to discriminate between military and civilian targets is in direct violation of international law—specifically, Protocol I, Article 51(4). The law places the responsibility for collateral damage resulting from disproportionate attacks on the party that failed to properly isolate military targets from noncombatants and civilian property. Protocol I, Article 51 further codifies the law of proportionality: “An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects … which would be excessive in relation to the concrete and direct military advantage anticipated [is to be considered indiscriminate].”

That is not to say civilians may never be targeted: a military decision maker must weigh potential civilian casualties, destruction of civilian property and the loss of indispensable civilian items against the benefit of achieving a military objective. However, complementing and implicit in the principle of military necessity is the principle of humanity. This principle forbids the infliction of suffering, injury or destruction not actually necessary for the accomplishment of legitimate military purposes. The principle of humanity itself is derived from the Martens Clause, providing that combatants “remain under the protection and the rule of the principles of the law of nations,” derived from the usages established by the dictates of public conscience.

Therefore, unless a cyber attack undertaken by the state during an armed conflict is precise enough to distinguish between civilian and military objects and—more significantly—effectively isolate the resulting harm to those targets to an acceptable degree, it would not be a permissible use of force during times of war. Finally, we must consider whether such a computer-based attack would be permissible during times of peace.

IV. PEACETIME CYBER ATTACKS

Generally speaking, the U.N. Charter prohibits international intervention through the use of force. The definition of “force” could be interpreted strictly in accordance with the text, or with the broad object and purpose of the U.N. Charter. Although it remains a contentious issue, “force” may not be restricted to a traditional armed attack. For example, a cyber attack aimed at causing harm to property and humans can be “reasonably characterized as a use of armed force” that falls under the prohibition of Article 2(4). Conversely, an incident in which one state attempts to disrupt, deny, degrade or destroy information resident in computers and computer networks from another would generally not constitute a use of force.

A. Self-Defense in a Cyber Attack

In response to a use of force, states have two options: (1) self-defense; and/or (2) Chapter VII action by the Security Council. States have the right to engage in self-defense if the use of force against them rises to the level of an “armed attack.” The ordinary meaning of the term “armed” is “equipped with or carrying a weapon or weapons,” “involving the use of firearms” and “prepared to activate or explode.” An “attack” under international humanitarian law refers to a particular category of military operations: for example, Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions defines “attacks” as “acts of violence against the adversary, whether in offence or in defense.” Though a computer is neither a weapon nor firearm, a cyber attack that results in an explosion or similar act of violence could be termed an “armed attack” for the purposes of Article 51.

However, in the Nicaragua case, the ICJ recognized that there are “measures which do not constitute an armed attack but may nevertheless involve a use of force” and distinguished “the most grave forms of the use of force from other less grave forms.” The court cited supplying weapons and providing logistical support to a rebel group in another state as an example of a use of force that did not amount to an armed attack against that state. Similarly, a state providing hacking tools to a terrorist group in another state may constitute an impermissible
use of force, but not an armed attack. According to the 31st International Conference of the Red Cross and Red Crescent Society (ICRC) in 2011, "cyber operations do not fall within the definition of ‘attack’ as long as they do not result in physical destruction or when its effects are reversible."98

Another legal caveat for self-defense—particularly preemptive self-defense—is that the threat must be real, credible and create an imminent need to act in accordance with the Caroline doctrine.89 The Caroline doctrine established that there had to exist "a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation."90 No strict prohibition precludes preemptive government use of force as long as the perceived threat is demonstrated to be real and immediate, and the state adheres to the criteria of proportionality and necessity: "since the act justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."91 The imminent threat is a standard criterion developed by Daniel Webster as he litigated the Caroline affair.92

In other words, if a state were faced with an attack that did not occur in conjunction with, or as a prelude to, conventional military force, the state would be allowed to respond with force in self-defense only if the attack was intended to directly cause property destruction or physical injury.93 Similarly, at the ICRC Conference, the organization circulated a background paper noting that “acts of violence … [denote] physical force.”94 Nevertheless, “cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as ‘acts of violence’, i.e. as an attack in the sense of [international humanitarian law]” and result in the permissible use of self-defense.95

As with an armed conflict, a state’s use of armed force in response to a cyber attack must also comply with the principles of necessity and proportionality under customary international law.96 The principle of necessity requires that force must be used only as a last resort, when peaceful means cannot achieve the state’s overall aim.97 Proportionality extends this logic, prohibiting force if the scope and intensity of force is excessive in relation to the state’s actual or imminent danger.98 Yael Stein, the research director of The Israeli Information Center for Human Rights in the Occupied Territories, contends:

The argument that this policy affords the public a sense of revenge and retribution could serve to justify acts both illegal and immoral. Clearly, lawbreakers ought to be punished. Yet, no matter how horrific their deeds … they should be punished according to the law. [These] arguments could, in principle, justify the abolition of formal legal systems altogether.99

Though customary international law had previously accepted reprisal, retaliation and retribution as reasonable responses, these types of strikes are illegal under contemporary international law because they are punitive—rather than legitimate—actions of self-defense.100 Hence, a state may utilize a cyber attack in response to a use of force that rises to the level of an armed attack, so long as the act remains curtailed by the necessity of self-defense and is proportional in both gravity and scale.

B. Chapter VII Response to a Cyber Attack

Alternatively, the Security Council may authorize collective action to maintain or enforce international peace and security.101 Specifically, the United Nations’ Charter authorizes the Security Council to investigate any situation threatening international peace; recommend procedures for peaceful resolution of a dispute; call upon other member nations to completely or partially interrupt economic relations as well as sea, air, postal and radio communications; or to sever diplomatic relations and enforce its decisions militarily, or by any means necessary.102

Therefore, cyber attacks attributable to the state that are reasonably expected to cause injury or death to persons or damage or destruction to objects are impermissible under international law outside of a recognized armed conflict. Even then, a state’s response to a cyber attack that rises to the level of an “armed attack” must be restrained by the confines of necessity and proportionality under international law. All other cyber attacks would likely constitute a use of force in violation of Article 2(4) and result in action by the United Nation’s Security Council. However, that analysis is beyond the scope of this article.

V. CONCLUSION

Recently, the United Nations’ Group of Governmental Experts agreed to initiate international rules of cyberspace for both peace and wartime.103 However, excluded from the consensus document was a U.S.-sponsored proposal to identify the implications of a 2013 experts’ group agreement that international law generally applies in cyberspace just as it does on land or at sea.104 Specifically, the U.S. wanted to include a citation to Article 51 of the U.N. Charter to legitimize a military response to an attack that caused death and destruction.105 As a result of the objections, the experts’ group ultimately agreed to
workaround language that endorsed the essence of Article 51, without explicitly referencing the document.106

The current state of international politics, with the demise of the Soviet Union as a superpower and the United Nations coalition victory in the 1991 Gulf War, has created a situation where non-conventional means offer the best mechanism to attack advanced “Western” countries.107 The Chinese, with their vast state-owned enterprises often run by the People’s Liberation Army, have argued that economic security and national security are one when it comes to the offensive use of cyber weapons.108 China is one of a limited number of countries whose military is specifically and openly exploring the incorporation of computer attacks into its broader military doctrine and strategy.109 In fact, the Chinese government has gone so far as to contemplate the development of a fourth branch of its military dedicated to computer and Information Warfare (IW), as well as recruiting civilian hackers and training them at army schools to create a cadre of “cyber warriors.”110

By comparison, the Council of Europe and the U.S. hold that these types of activities constitute criminal acts.111 During his campaign, former President Obama stated that: “We must urgently seek to reduce the risks from three potentially catastrophic threats: nuclear weapons, biological attacks, and cyber warfare.”112 On April 1, 2015, President Obama issued an Executive Order establishing the first-ever economic sanctions program in response to cyber attacks.113 According to the Order, individuals and entities responsible for cyber attacks that threaten the national security, foreign policy, economic health or financial stability of the U.S. will have their assets frozen by the Treasury Department.14

Before the infamous Russian election-meddling scandal, General Valery Gerasimov, chief of staff of the Russian Armed Forces, published an article in a military trade magazine describing a change in doctrine from large-scale traditional warfare to a hybrid, “asymmetrical” approach that effectively hacks an enemy’s society rather than carries out a direct physical attack:

Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The very ‘rules of war’ have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.115

Cyber technologies and infrastructure—from satellites to smart phones—play an increasingly indispensable role in daily life. At the same time, threats to cyber security are becoming both more numerous and more serious.116

The failure of the international community and this country to address these concerns in a united and consistent manner is a threat to every technologically-dependent nation on the planet. Perhaps the responsibility falls on the civilians, then, to pressure their governments to adopt these general guidelines into reasonable, well-defined and enforceable law—law that transcends borders for the sake of us all.

ENDNOTES


5 Some common cyber attack weapons include: (1) “Sniffer,” a program executed from a remote site by an intruder, which allows the intruder to retrieve user identification and passwords; (2) “Trojan Horse,” a program which misrepresents itself as useful, routine or interesting to persuade a victim to install it; (3) “Trap Door,” a program used to gain unauthorized access into secured systems; (4) “Logic Bomb,” a program that lies dormant until a trigger condition causes it to activate and destroy the host computer’s files; (5) “denial of service” attacks, which prevent networks from exchanging data; (6) “computer worm” or “computer virus” attacks, which travel from computer to computer, damaging files; and (7) spamming, which floods military and civil e-mail communications systems

* Anna C. Mourlam is an associate at Perkins Coie LLP, where she represents international and domestic businesses across a wide range of industries and stages of growth. She is a member of the commercial litigation practice group, and handles matters including data security and privacy; securities and enforcement; and white-collar criminal defense. A graduate of Northwestern University and Notre Dame Law School, Ms. Mourlam has frequently published on the topics of cybersecurity, transnational trade regulation and corporate compliance.


8 Shields, supra n.7; Naylor, supra n.7.


10 The Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism was developed as a follow-up to a conference hosted at Stanford University in 1999. Members of government, industry, NGOs and academia from many nations met to discuss the growing problem of cybercrime and terrorism. A clear consensus emerged that greater international cooperation was required, and considerable agreement that a multilateral treaty focused on criminal abuse of cyber systems would help build the necessary cooperative framework. See Sofera, supra note 4.


13 The text and commentary of Additional Protocol I support this conclusion. For example, the rules of proportionality speak of the “loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof.” See Part III of this article. Wartime Cyber Attacks.

14 The effects principle is born out of the Case of the S.S. “Lotus,” or Lotus decision. There, a criminal trial resulted from the collision between the S.S. Lotus, a French steamship, and the S.S. Boz-Kurt, a Turkish steamship, in a region just north of Greece on August 2, 1926. As a result of the accident, eight Turkish nationals aboard the Boz-Kurt drowned when the vessel was torn apart by the Lotus. The Lotus principle or Lotus approach, commonly considered a foundation of international law, says that sovereign states may act in any way they wish so long as they do not contravene an explicit prohibition. See The Case of the S.S. “Lotus” (France v. Turkey), Permanent Ct. of Int’l Just., Judgment 1927 P.C.I. (ser. A) No. 10 (Sept. 7).

15 See 22 U.S.C. § 6801(9); see also Restatement (Third) of Foreign Rel. § 402(f)(c) (1987).


17 See Corfu Channel, Judgment, 1949 I.C.J. 4, ¶ 22 (Apr. 9); see also Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), Principle 1, ¶ 9, U.N. Doc. A/8082 (Oct. 24, 1970) (imposing a duty upon countries “to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in such acts”).

18 See Corfu Channel, supra note 17; see also, Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 31-32 (June 27); Velásquez Rodríguez v. Honduras case, Inter-American Court of Human Rights, Series C, No. 4, ¶ 170 (1988) (“[U]nder international law a State is responsible for the acts of its agents undertaken in their official capacity and for their omissions”).


22 See Schmitt, supra note 12, at 34.

23 Id. at 36.


25 Id. at ¶¶ 63-64.

26 Id. at ¶ 29.


28 Therefore, actions by private individuals may be attributable where a state fails to exercise reasonable diligence to prevent intentionally wrongful conduct that it knows or should know is very likely to occur. See Scott J. Shackelford, State Responsibility for Cyber Attacks: Comparing Standards for a Growing Problem, Conference on Cyber Conflict 203 (2010); see also Zaitro Case (Gr. Brit. v. US), 6 RIAA 160, 163-64 (1925); Spanish Zone of Morocco (Gr. Brit. v. Spain), 2 RIAA 615, 642-43 (1923); Malcolm Shaw, Int’l Law 568 (1997).

29 This is true even if the conduct itself occurs outside the state’s borders.

30 That is, merely funding a group engaged in operations against another state does not reach the threshold for the state’s use of force. See Military and Paramilitary Activities in and Against Nicaragua, supra note 18, at ¶¶ 62, 110, 228.

For example, when Israeli forces utilized deception—disguising their military effort. An attack that has no reasonable connection to the conflict at hand would be examined under separate international law. \( \text{i.d. at 76;} \) see also Part IV of this article. Peacetime Cyber Attacks.


35 See 1 International Committee of the Red Cross, Rule 3: Definition of Combatants, CUSTOMARY INT'L HUM. HUMANITARIAN L. (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005), https://www.icrc.org/customary-ih/en/docs/v1_rul_rule3 (“[E.g., the military manuals of Argentina (ibid., § 574), Australia (ibid., § 575), Belgium (ibid., § 576), Benin (ibid., § 577), Cameroon (ibid., § 578), Canada (ibid., § 579), Colombia (ibid., § 580), Croatia (ibid., §§ 581-82), Dominican Republic (ibid., § 583), Ecuador (ibid., § 584), France (ibid., §§ 585-86), Germany (ibid., § 587), Hungary (ibid., § 588), Indonesia (ibid., § 589), Israel (ibid., § 590), Italy (ibid., §§ 591-92), Kenya (ibid., § 593), South Korea (ibid., § 594), Madagascar (ibid., § 595), Netherlands (ibid., § 596), New Zealand (ibid., § 597), Russia (ibid., § 598), South Africa (ibid., § 599), Spain (ibid., § 600), Sweden (ibid., § 601), Togo (ibid., § 602), United Kingdom (ibid., § 603) and United States (ibid., §§ 604-06”)”); see also Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol I) art. 43, June 8, 1977, 1125 U.N.T.S. 3. Additionally, combatants must follow laws of war, but failing to do so does not remove their “combatant” status. Protocol Additional to the Geneva Conventions at art. 44; see also Hague Convention No. III Relative to the Opening of Hostilities art. 1, Oct. 18, 1907, 36 Stat. 2259, 2271 T.S. 598 (1907).


37 See Yael Stein, By Any Name Illegal and Immoral, 17(1) ETHICS & INT'L AFFAIRS 127, 129 (2003).

38 For example, when Israeli forces utilized deception—disguising themselves as women or Arabs to facilitate getting to Palestinian targets—they were in violation of this law. See George H. Aldrich, The Taliban, Al Qaeda, and the Determination of Illegal Combatants, 96 AM. J. INT'L L. 891 (2002); see also Stein, supra note 37, at 137.


40 Id.


42 See Stein, supra note 37, at 129.


44 Id.

45 Id.

46 Id.


48 Whereas many special tasks identified by armbands are listed in regulations, e.g., military police, gas experts, photographers and personnel protected under the Geneva Conventions, no provision for armbands is made in U.S. Army Regulation. \( \text{i.d.} \)

49 Many Internet interactions are memorialized only by computers’ exchange of unique numeric identifiers, called Internet Protocol (IP) addresses, assigned to them by their respective Internet Service Provider (ISP). Although it is theoretically possible to determine which user was assigned which IP address, there are a number of practical obstacles to overcome. To begin, an ISP normally controls a range of hundreds or thousands of IP addresses, assigned to customers either “dynamically” or “statically.” In the case of dynamic assignment, each time the user accesses the ISP to connect to the Internet, the ISP assigns one of the available IP addresses to the customer’s computer for the duration of the customer’s session (i.e., until he or she disconnects). Each time the customer connects to the Internet, the user may receive a different IP address. By contrast, a user with a static IP address commonly has a permanent, 24-hour Internet connection and an IP address that remains constant over weeks or months. See Todd M. Hinnen, The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet, 5 COLUM. SCI. & TECH. L. REV. 1, 5 (2004).

50 After all, anonymity is the hallmark of cyber attacks.

51 See Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 MIL. L. REV. 1, 74-75 (2009); Jeffrey Carr, Inside CYBER WARFARE 29 (2010) (“Hacking attacks cloaked in nationalism are not only not prosecuted by Russian authorities, but they are encouraged through their proxies, the Russian youth organizations and the Foundation for Effective Policy.”).

52 However, the United States has never officially acknowledged its role in the attack. See Kim Zetter, Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force,’ WIRED (Mar. 25, 2013), http://www.wired.com/2013/03/stuxnet-act-of-force/.

53 Until the attacks occurred, intelligence agencies speculated that Iran would be able to produce a nuclear weapon by 2010. \( \text{i.d.} \)

54 The Chatham House’s Principles of International Law on the Use of Force by States in Self-Defence defines an armed attack as “an intentional intervention in or against another State without that State’s consent or subsequent acquiescence, which is not legally justified.” The matter was raised particularly by the Oil Platforms judgment, which quoted a famous passage of the Nicaragua case: “It is necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.” There, three Iranian offshore oil platforms and a United States Navy warship were destroyed when the ship struck a mine in international waters near Bahrain. The Oil Platforms case denied the argument made by the United States that an accumulation of events of smaller scale could amount to an armed attack of grave proportions capable of triggering the right of self-defense. Therefore, in the cyber context, the use of force would have to be of “grave proportions” to amount to an armed attack and allow for retaliation. See Elizabeth

27 VOL. 26, NO. 1, WINTER 2018 • WWW.CALAWYERS.ORG/INTERNATIONAL • THE CALIFORNIA INTERNATIONAL LAW JOURNAL
The prohibition on attacking civilian objects has historical roots in the 1868 St. Petersburg Declaration, which provided that “the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy.” See St. Petersburg Declaration, preamble; see also Hague Convention No. IV Respecting the Laws and Customs of War on Land, with Annex of Regulations, Oct. 18, 1907, art. 25, 36 Stat. 2277, T.S. 398 (1907) (“The attack or bombardment...of towns, villages, dwellings, or buildings which are undefended is prohibited”); Joyner & Lorrionde, supra note 5, at 850.

57 The prohibition on attacking civilian objects has historical roots in the 1868 St. Petersburg Declaration, which provided that “the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy.” See St. Petersburg Declaration, preamble; see also Hague Convention No. IV Respecting the Laws and Customs of War on Land, with Annex of Regulations, Oct. 18, 1907, art. 25, 36 Stat. 2277, T.S. 398 (1907) (“The attack or bombardment...of towns, villages, dwellings, or buildings which are undefended is prohibited”); Joyner & Lorrionde, supra note 5, at 850.


61 Id.

62 Id.

63 Id.

64 Id.

65 See Critical Foundations: Protecting America’s Infrastructure, supra note 2, at 25-3, 1-1 (setting forth the five critical infrastructures whose incapacity or destruction would have a debilitating effect on U.S. defense or economic security); see also Brian A. Persico, Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure, 7 COMMUNICATIONS & CONSENT 153, 156-60 (1999) (classifying the Information and Communications infrastructure to include telephone networks, internet and personal computers; the Physical Distribution infrastructure to encompass the vast network of highways, rail lines, ports, pipelines, inland waterways, airports and air traffic control systems found throughout the United States; the Energy infrastructure to include electric power systems, oil and gas refining and transmission facilities in the United States; the Banking and Finance infrastructure to include banks, financial services companies, payment systems, investment companies and securities and commodities exchanges; and the Vital Human Services infrastructure to consist of the water supply, emergency services and government services of the United States).

66 See Protocol Additional to the Geneva Conventions, supra note 35.

67 Id. at art. 52.2. See also, International Committee of the Red Cross, 31st International Conference of the Red Cross and the Red Crescent, Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report 31HC/11/5.1.2 (Oct. 10, 2011) (“By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way.”).

68 Article 52.2 of Protocol I states that, “military objectives are limited to objects that are effective contributions to military action and whose destruction offers a military advantage.” Protocol Additional to the Geneva Conventions, supra note 35.

69 Thus, only measures that are “indispensable for securing the complete submission of the enemy as soon as possible” should be undertaken. See U.S. Army Law Of War HANDBOOK 164 (Maj. Keith E. Pulz ed., 2005).


71 “Indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.” Id. at art. 51(4); see also Schmitt, supra note 12, at 110 (“The principle of distinction applies to cyber attacks.”).

72 See W. J. Fenrick, Targeting and Proportionality During the NATO Bombing Campaign Against Yugoslavia, 12 EUR. J. INT’L L. 489 (2001); see also Schmitt, supra note 12, at 152 (“Additional Protocol I prohibits States Parties from making the civilian population, individual civilians, civilian objects, cultural objects and places of worship, objects indispensable to the survival of the civilian population, the natural environment, and dams, dykes, and nuclear electrical generating stations the object of a cyber attack by way of reprisal.”).

73 See Protocol Additional to the Geneva Conventions, supra note 35.

74 After deciding that the target is a military objective, the elements of the balancing test include “target selection, the means and methods chosen for the military strike, the lack of negligence in the execution of the military strike, and the determination of what constitutes the military advantage of a particular military strike.” Randy W. Stone, Protecting Civilians During Operation Allied Force: The Enduring Importance of the Proportional Response and NATO’s Use of Armed Force in Kosovo, 50 CATH. U. L. REV. 501, 522 (2001).


77 The Martens Clause is contained in the preamble to the Hague Convention IV of 1907. See A. Rogers, LAW ON THE
The gravity of the attack depends on several factors, such as: severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy. However, these factors are not exhaustive. See infra note 22, at 45, 48-51 (“A cyberspace autonomy utilizes a force of which its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”).


The Caroline incident involved British troops crossing U.S. borders to destroy an enemy vessel. Britain justified the action on the grounds that the U.S. was not enforcing its laws along the frontier, and that the action was a legitimate exercise of self-defense. See Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), reprinted in 2 John Moore Dig. of Int’l Law 409-11 (1906).

See Schmitt, supra note 80, at 903, 909 (evaluating whether a cyber attack rises to the level of an armed attack based on: (1) severity, the type and scale of the harm; (2) immediacy, how quickly the harm materializes after the attack; (3) directness, the length of the causal chain between the attack and the harm; (4) invasiveness, the degree to which the attack penetrates the victim state’s territory; (5) measurability, the degree to which the harm can be quantified; and (6) presumptive legitimacy, the weight given to the fact that, in the field of cyber-activities as a whole, cyber attacks constituting an armed attack are the exception rather than the rule).

See International Committee of the Red Cross, supra note 67.

Id.; see also 18 U.S.C. § 1030(c)(8) (defining “damage” as “any impairment to the integrity or availability of data, a program, a system, or information” that (A) causes loss aggregating at least $5,000 in value during any one-year period to one or more individuals; (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (C) causes physical injury to any person; or (D) threatens public health and safety).


See R.Y. Jennings, The Caroline and McDondall Cases, 32 Am. J. Int’l L. 82, 89 (1938) (quoting Secretary of State Daniel Webster’s letter to his British counterpart concerning the Caroline incident: “It must be shown that admonition or remonstrance to the persons on board the Caroline was impracticable, or would have been unavailing… but that there was a necessity, present and inevitable, for attacking her…”).

See Robert D. Sloane, The Cost of Conflation: Preserving the Dualism of Jus Ad Bellum and Jus in Bello in the Contemporary Law of War, 34 Yale J. Int’l L. 47, 108-09 (2009). Note, the United States has acknowledged that these principles apply to cyber-attacks. See, e.g., International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World, White House 4 (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (“[W]e will exhaust all options before military force whenever we can; will carefully weight the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.”).

See Stein, supra note 37, at 129-37.

Reprisal allows a state to commit an act that is otherwise illegal to counter the illegal act of another state. Retaliation is the infliction upon the delinquent state of the same injury that it has caused the victim. Retribution is a criminal law concept implying vengeance that is sometimes used loosely in the international law context as a synonym for retaliation. See Shaw, supra note 28, at 777-91; see also Derek Bowett, Self-Defence in International Law 13 (1958).


According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.

According to James Lewis, the experts’ group rapporteur and director of the Center for Strategic and International Studies’ Strategic Technologies Program, “The Chinese line was ‘we don’t want to say Article 51, because that would militarize cyberspace and that’s a zone of peace.’” Unspoken, however, was the concern that U.S. would use the provision to justify counteraction for harm such as the breach of millions of federal employee records at the Office of Personnel Management, an attack officials have anonymously attributed to China. Id.

That proposal was rebuffed by a coalition of nations—including Russia, China, Pakistan, Malaysia and Belarus—that argued the move would institutionalize U.S. hegemony in cyberspace. Id.
I. INTRODUCTION

When faced with a choice between privacy and convenience, most individuals often, albeit unwittingly, choose the latter over the former. It appears that privacy is the price individuals are willing to pay for convenience, and history has borne witness to this fact. Despite the absence of privacy, individuals historically embraced (then) novel means of communication on account of the convenience they provided. The 1870s saw a shift from the use of sealed letters to less private but more convenient postcards. During the early 20th century, people welcomed shared technology by using telephones with party lines in lieu of individual telephone lines. In the present internet age, individuals willingly “partake in the offerings of the internet and participate in what has become one of the most important social spheres.” Evidently, privacy in the realm of technological innovation is perceived to be far less important than ostensible benefits made available by technology.

The most recent iteration of the choice of convenience over privacy in the realm of communication relates to the Internet of Things (IoT), defined as “a network that connects uniquely identifiable Things to the Internet, [which] have sensing [or] actuation and potential programmability capabilities.” A beacon of convenience, the IoT allows “billions of digital devices, from smartphones to sensors in homes, cars, and machines of all kinds, to communicate with each other to automate tasks and make life better.” It monitors users’ everyday lives by collecting information, and consequently claims to improve said lives through automation by streamlining daily and routine tasks. It likewise creates possibilities to “improve energy conservation, efficiency, productivity, public safety, health, education and more,” thus aiding in the development of “new economic and social opportunities” in an interconnected world. The IoT has also disrupted everyday lives by encouraging connectivity through “a variety of cool and mundane objects that people interact with” as opposed to interacting with each other.

But behind the smoke and mirrors of the IoT and the convenience it purportedly offers lie serious concerns regarding security and privacy. To achieve the connectivity and efficiency it promises, the IoT collects unparalleled amounts of data regarding users’ personal lives. The technology within the IoT gathers data and “provides for a real-time application of data processing, data storage, and data analysis.” In fact, the IoT has effectively changed the notion of privacy. By design, it is “a system of surveillance,” which “has the potential to generate an almost inescapable data web that monitors many aspects of [users’] lives.” This runs counter to human behavior in our society; people typically exclude strangers from entering their homes or private spaces for fear of invasions to their privacy or risk of harm to their safety and security. However, people knowingly and willingly place IoT devices inside their homes, referred to as Home Internet of Things (Home IoT) devices. They willingly purchase these devices for convenience wrapped in “cool” technology, but, in reality, they have let strangers inside their most private spaces, allowed them to listen to their most private conversations and even welcomed them inside their own thoughts.

The preference for convenience is also manifested in the response to lengthy contracts in the form of terms and conditions, or licenses in the guise of operating manuals that accompany Home IoT devices. People scroll over these contractual documents as quickly as possible, or sometimes not at all, to access a website or to use a new technological gadget without a second thought as to the need to protect their personal privacy. This behavior may have arisen from the ambiguity and one-sidedness of such form contracts, which people encounter on a frequent basis. The recent Facebook and Cambridge Analytica fiasco is an example. Facebook’s user data was collected through a personality quiz and later sold to the political firm Cambridge Analytica. In Congressional
hearingsthe Terms of Use of the leading technology giant Facebook were criticized for being too difficult for average users to comprehend.\textsuperscript{15} The contract was also deemed too one-sided in favor of Facebook.\textsuperscript{16} In other words, the incomprehensibility of the Terms of Use could have led Facebook’s users to give up on any attempts to read and understand the contract, and instead encouraged them to simply agree with the one-sided contractual provisions as they were written. It is likely that technology manufacturers are taking advantage of individuals’ strong preference for convenience.

This article seeks to address the way in which Home IoTs, specifically those with recording capabilities, invade an individual’s sphere of privacy. The invasive nature of Home IoTs is considered in light of the consent-based approach of, and principles on the lawful processing of data espoused in, the European Union General Data Protection Regulation (GDPR or Regulation), as well as the sector-specific data privacy protection framework of the U.S., with a particular focus on the State of California. The article will also examine contractual abuses resulting from contracts of adhesion and data ownership issues arising from Home IoTs and related data breaches.

This article is structured as follows: Part II discusses the interconnected nature of Home IoTs and related risks. Part III focuses on the contracts that govern the use of Home IoTs, which expand the individual’s sphere of privacy, albeit unwittingly, and attempt to change the rules of ownership. Part IV briefly introduces the GDPR and explores its consent-based approach for protection of personal data; it also examines the sector-specific framework of relevant U.S. privacy-related laws, and their effects on the use of Home IoTs.

II. THE INTERCONNECTED NATURE OF HOME INTERNET OF THINGS

More commonly known as “smart objects,”\textsuperscript{17} the IoT encompasses an “intelligent, invisible network fabric”\textsuperscript{18} of everyday objects which are embedded with technology allowing them to connect and communicate with each other and the internet.\textsuperscript{19,20} The IoT movement has been well embraced by individuals to the point that the number of connected devices has exceeded the number of people.\textsuperscript{21}

A subset of the IoT comprises Home IoTs, which consist of devices specifically catered to home automation. These include “monitoring systems, smart appliances, and connected entertainment,”\textsuperscript{22} which allow people to control their homes at their own convenience.\textsuperscript{23} Through optimal use and proper programming, home automation contributes to improved efficiencies,\textsuperscript{24} reduced costs and conservation of energy.\textsuperscript{25} However, by allowing these devices to control home environments, people are also permitting them to collect, transmit and analyze data about their way of life.

This is made easier through Home IoTs with recording capabilities or smart speakers such as Amazon’s Alexa, Google Home and Apple HomePod (Home IoT Smart Speakers), which allow individuals to instruct them to perform certain tasks and to control other Home IoT devices.\textsuperscript{26} These devices are trained in vocal recognition to respond to instructions to provide personalized results.\textsuperscript{27} However, an underlying aspect of vocal recognition is listening and, consequently, recording any information and conversations made within the devices’ vicinity.\textsuperscript{28} Although the information gathered is used “to improve the accuracy of the results provided to [individuals] and to improve [the] services [provided],”\textsuperscript{29} the information may likewise be used for nefarious purposes which ultimately compromises privacy and security.

The growing risk of Home IoTs is manifested in security and privacy concerns surrounding the use of these devices. Security considerations primarily arise due to poorly secured devices,\textsuperscript{30} which “enable[s] unauthorized access and misuse of personal information, facilitate[s] attacks on other systems, and create[s] physical safety risks.”\textsuperscript{31} The lack, or absence, of strong and reliable security features acts as an entry point for cyberattacks.\textsuperscript{32}

The nature of interconnectivity and promise of convenience likewise increase security risks. Home automation encourages individuals to use several Home IoTs in their homes to maximize the benefits of interconnectivity. This results in an “increase[d] … number of vulnerabilities” which cyber attackers may target to attack network systems and remotely control Home IoTs.\textsuperscript{33} The same interconnectivity which offers convenience poses a danger\textsuperscript{34} by inviting potential attackers to access and steal massive amounts of information\textsuperscript{35} for identity theft, and to compromise access points with the goal of spying on individuals or attacking third parties.\textsuperscript{36}

Home IoT Smart Speakers, in particular, are most vulnerable to eavesdropping and unauthorized conversation attacks.\textsuperscript{37} Eavesdropping, also termed “sniffing,” is defined as “intentionally listening to private conversations over the communication links.”\textsuperscript{38} The listening and recording features of Home IoTs in the form of smart speakers allow cyber attackers to access and process “captured information to design other tailored attacks.”\textsuperscript{39} Unauthorized conversation refers to the connective and communicative ability of Home IoTs to acquire and share information with other Home IoTs which may result in the “control of the whole home automation
Another prevalent concern is the invasive nature of Home IoTs on individuals’ privacy. As a concept, privacy pertains to “confidential aspects of life, control of one’s own public profile and a life free of unwarranted interference.” The IoT movement has drastic effects on privacy arising from the sheer amount of data collected, retained and analyzed. The information accumulated by these devices encompasses data about an individual’s lifestyle, preferences, location and daily habits. When aggregated, the available data “paint detailed digital portraits” of individuals. These pieces of personal information, whether aggregated or not, may be sold to third parties so as to arm them with tools to understand their markets, or worse, for surveillance purposes. The commercialization of personal information is a grave form of invasion of individual privacy since it allows manufacturers and third parties, who have been granted access, to extract patterns in human behavior and preferences which are often perceived to be of high value. Dire consequences arising from this phenomenon include preconceived discrimination and misuse and abuse of data.

With regard to Home IoT Smart Speakers, every instruction and command to these devices translates to behavioral data collected about individuals, which may be sold and utilized for marketing purposes. Further, their ability to listen and record instructions and conversations likewise poses an increased risk of spying or wiretapping. These blatant invasions of privacy violate the sanctity of the sphere of privacy.

Despite their convenience, Home IoTs also come with significant risks with potential far-reaching consequences that raise concerns about the commercialization of individuals’ private information and abuse of data gathered.

### III. HOME INTERNET OF THINGS AND THE SHIFT OF DATA OWNERSHIP BY MEANS OF CONTRACTS OF ADHESION

The act of bringing Home IoTs into individuals’ homes under the guise of convenience is tantamount to inviting Home IoT manufacturers to collect, transmit, analyze and capitalize on customers’ personal information based on their “purchasing habits, preferences, and daily routines.” Individuals have effectively permitted Home IoT manufacturers to gain “unprecedented access to immense amounts of electronic data” to the detriment of their personal privacy. However, Home IoT manufacturers have gone a step further. Like a thief in the night, Home IoTs have been silently shifting the rules of data ownership.

While the rules as to ownership of data gathered by Home IoT devices are unclear, many, if not all, Home IoT manufacturers have claimed ownership over any or all information they have collected through the use of such devices.

Much significance is attached to ownership of data derived from the use of Home IoT devices. Control over any activity concerning data stems from ownership. Without a clear indication of ownership, Home IoT manufacturers are free to engage in the commercialization of gathered data, whether in singular or aggregated form.

Home IoT manufacturers take advantage of lengthy and obscure Terms and Conditions and Privacy Policies by “includ[ing] contracting terms that, at the very least, skew in the company’s favor, or, at the very worst, include contractual abuse.” Further, individuals’ strong preference for convenience, as manifested by their easy acquiescence, is likewise a contributing factor since they tend to simply gloss over or completely ignore these contracts.

The claim of ownership over consumer data is usually couched in obscure legalalese and embedded deep within Home IoTs’ Terms and Conditions. Terms and Conditions are electronic contracts which are “distance contract[s] concluded between absent parties which, as in any other contract, involve[] the exchange of consents between contracting parties with the intention to establish, modify, or extinguish a specific legal relationship.” These often take the form of contracts of adhesion which contain clauses governing the use and ownership of goods and services imposed by the manufacturer or service provider.

Contracts of adhesion are essentially “take it or leave it” contracts where negotiation of contractual terms is not entered into or even considered. These are usually drafted by the party in a stronger position. The weaker party may either agree to the terms as drafted, or reject the terms, thereby losing access to the use of Home IoT device. Left with not much of a choice, at least 90% of individuals, as determined in a recent survey, agree to Terms and Conditions without actually reading their contents, in exchange for access.

While it appears that technology has propelled the use of contracts of adhesion, this form of contracting is not novel. Contracts of adhesion were initially developed to address arm’s-length exchanges during the early rise of capitalism and were
eventually embraced “due to their efficient and utilitarian function.” The rise of technology ushered in the era of shrink-wrap agreements, which retain the essential features of contracts of adhesion. Shrink-wrap agreements, which earned their moniker from the plastic wrap encasing software stored in physical media, likewise “impose[] restrictions on use, reproduction, transfer, and modification of the software program by the consumer.” The idea behind shrink-wrap agreements is that the potential user should read the pre-printed form encased by the shrink-wrap prior to opening the package. Should he or she acquiesce to the Terms and Conditions, which often include strict licensing terms in favor of the manufacturer, then he or she proceeds to break the shrink-wrap. However, unbeknownst to the unwitting consumer, the tearing of the shrink-wrap signifies assent to the contractual terms drafted by the manufacturer. This puts the user in an unfortunate position which may result in relinquishment of any ownership rights over the software program, or perhaps of any data which he or she may input in the process of using the program.

Other forms of contracts of adhesion as enhanced by technology are the browse-wrap agreement and the click-wrap agreement. The browse-wrap agreement binds users based on the mere fact that they have been given the opportunity to browse through the Terms and Conditions. The agreement usually hides behind a link placed on an obscure part of a manufacturer’s website. It presumes that a user has agreed to and has accepted the Terms and Conditions through mere usage. This effectively disregards individual users’ power of giving active consent.

Click-wrap agreements, otherwise referred to as clickthrough agreements, are “contract[s] of adhesion for the conclusion of which the service recipient of an offer made online (via Internet) has just to tick a box (make a simple click on an icon), the ‘Yes’ or ‘I accept’ or ‘I agree’ or other similar button.” A user is deemed to have assented to the Terms and Conditions by clicking “I agree.” This provides a more apparent manifestation of consent since some sort of signifier is required on the part of the user. However, the user remains powerless in his or her ability to negotiate any part of the contract. The user is effectively left with no choice but to agree and accept the Terms and Conditions should he or she wish to use the good or service.

The above contracts of adhesion, regardless of how they are named, often share the same characteristics that cause individual users to pass through or do away with reading them. Simply put, individual users enjoy a strong preference for convenience and manufacturers take advantage of this by capitalizing on the use of contracts of adhesion. Terms and Conditions are “notoriously difficult to understand” because of “opaque wording” unfamiliar to the ordinary user who understands neither legalese nor “a plethora of technological terms.” Further, most Terms and Conditions are designed and written based on “previous states of technological development” which renders them unsuitable for newer forms of technology.

Another concern is that many provisions governing use and ownership are scattered throughout several contracts. This renders the Terms and Conditions difficult to read, interpret and understand for the average individual user. Consequently, most individual users are “completely unaware” that they may have waived rights, including ownership and use, over their data. It is highly likely that waiver leads to the intentional sharing of data to third parties who unscrupulously sell the data to the highest bidder.

Home IoT manufacturers maximize the advantage that legally permissible contracts of adhesion allow. Individual users signify their assent to one-sided contractual provisions by merely browsing or clicking through Terms and Conditions that govern the use and ownership of Home IoT devices and any data collected or generated. Assuming individual users do read the contracts of adhesion, they are not presented with “a realistic opportunity to bargain” since the acquisition or use of the product or service may only be acquired if one agrees to the contractual provision. As a result, individual users have waived their personal privacy as to any data they share with Home IoT devices and make available in their homes, thus significantly reducing their sphere of privacy. This engenders potential abuses with regard to privacy, placing the individual user in a perilous position. In fact, “in most aspects, [privacy] has already been compromised almost beyond repair.”

IV. EXISTING PRIVACY LAWS AND FRAMEWORKS ARE INSUFFICIENT TO PROTECT PRIVACY

In light of security and privacy concerns in the digital era, regulators have attempted to develop protective and preventative mechanisms to guard against potential abuses of individuals’ personal privacy. Establishing rules on privacy and security is paramount to building trust to protect one’s data and identity in the face of new and constantly evolving technological developments.

A. The Consent-Based Approach of the EU General Data Protection Regulation as Insufficient Means of Protecting Privacy

The leading legislation on privacy is the European Union’s General Data Protection Regulation (GDPR), which builds on the principles established by Data Protection Directive 95/46/
The GDPR aims “to harmonize data privacy laws” in the European Union for the protection of all of its individual members. Approved by the European Parliament on April 14, 2016, the GDPR took effect on May 25, 2018.

The GDPR acknowledges that “rapid technological developments and globalisation have brought new challenges for the protection of personal data,” such as the increased scale of collection and sharing of personal data. It likewise recognizes the double-edged sword of technology. On one hand, technology is integral to the economy and society, but on the other hand, it also permits abuses of personal data “on an unprecedented scale” for the benefit of corporations and state authorities. The GDPR strives to achieve the balance of “facilitating the free flow of personal data … while ensuring a high level of the protection of personal data.”

The GDPR casts a wide net in terms of its scope of protection. Though seemingly limited to the protection of personal data within the European Union, the GDPR’s expansive scope affects individuals and corporations on a global scale. Its territorial scope operates broadly and involves data subjects and controllers outside the European Union. The provisions of the GDPR apply when: the data controller is based in the European Union; and the data controller, even if established elsewhere, offers goods and services to individuals inside the European Union regardless of where the processing occurs; the provisions of the GDPR apply when: the data controller is based in the European Union; and the data controller, even if established elsewhere, offers goods and services to individuals inside the European Union; and the data controller, even if established elsewhere, monitors the behavior of individuals within the European Union.

This effectively guards individuals’ personal data against unscrupulous processors who collect personal data of individuals within the European Union with the aim of escaping the reach of the GDPR by processing the data elsewhere.

The GDPR defines “personal data” as “any information relating to a identified or identifiable natural person,” who is also referred to as the data subject. The information collected by Home IoT manufacturers and their corresponding devices from individual users is considered personal data. The data collected allow Home IoT devices to associate certain results that are more attuned to the preferences of individual users. In effect, Home IoT devices provide a more effective response to the specific needs of an individual user. Under the GDPR, a controller refers to the person or entity who “determines the purposes and means of the processing of personal data,” and a processor is one who “processes personal data on behalf of the controller.” Home IoT manufacturers, as controllers, and their designated processors have a responsibility to comply with the rules of the GDPR. Failure to do so will result in penalties, the most severe of which is an administrative fine of “up to €20 million [approximately USD 23M] or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”

The GDPR primarily illustrates a consent-based approach to protecting personal data. The use of an individual’s personal data is highly dependent on whether he or she has granted consent to the processor or controller of personal data. In fact, absent any legitimate legal basis, lawful processing of personal data is based on the consent of the individual user. Under the Recitals of the GDPR, much significance is placed on the value of consent, to wit:

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
However, the fact remains that individual users may contract away the ownership and use of their personal data, whether in singular or aggregated form, to third parties. As discussed, this is usually achieved by Home IoT manufacturers through Terms and Conditions in the form of contracts of adhesion. The GDPR seeks to protect individual users by prescribing strict rules as to acquisition of consent. By doing so, it effectively shifts accountability over personal data to controllers and processors.

To protect the interest and privacy of individual users, the GDPR advances conditions for valid consent. The conditions show that the controller bears the responsibility for ensuring that consent has been given in accordance with the requirements of the GDPR. It likewise provides safeguards against collecting data unnecessary for the fulfillment of relevant contracts. In this regard, Home IoT manufacturers are prevented from collecting personal data though their devices that are deemed excessive to the fulfillment of their services. By requiring the use of “clear and plain language,” the GDPR prevents Home IoT manufacturers from obscuring the needless collection of excessive and unnecessary personal data in ambiguous Terms and Conditions.

In addition, the GDPR sets forth governing principles to ensure lawful processing of data on the part of actors such as Home IoT manufacturers. These principles are lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. Under these principles, it is incumbent upon Home IoT manufacturers, as data controllers, and their designated data processors, to be conscientious in the responsible collection, analysis and transfer of individual users’ data. These principles ensure that Home IoT manufacturers can no longer hide behind one-sided and unfathomable Terms and Conditions to the detriment of the individual user.

Under the first principle of lawfulness, fairness and transparency, Home IoT manufacturers should warrant that “any information and communication relating to the processing of [those] personal data [should] be easily accessible and easy to understand.” As a result, Terms and Conditions should do away with complex terminologies and should be written in clear and plain language so as to ensure that average individual users understand the processing and the purpose behind it.

The second principle of purpose limitation requires Home IoT manufacturers to provide individual users with “specified, explicit and legitimate” purposes when collecting their personal data. Any personal data collected through Home IoT devices should stem from a concrete purpose as provided for in the Terms and Conditions. For that reason, Home IoT manufacturers should inform individual users as to why they seek to collect certain pieces of personal information, and of any consequences that may arise should the requested data not be given.

In line with the third principle of data minimization, the processing of data should not be excessive in relation to the purposes of which the individual users have been informed through the Terms and Conditions. Home IoT manufacturers bear the responsibility of collecting data within adequate, relevant and necessary means in relation to the stated purposes.

It is likewise essential for Home IoT manufacturers to guarantee that any data collected is “accurate and, where necessary, kept up to date.” If any changes occur, then these should be rectified in a timely manner. In addition, Home IoT manufacturers, and their designated processors, should be mindful of the storage limitation rule which requires that data be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.” This warrants that the rights and freedoms of individual users are safeguarded against security breaches instigated by Home IoT manufacturers’ actions or poor systems.

Lastly, the GDPR dictates that Home IoT manufacturers, and their corresponding processors, uphold integrity and confidentiality in their data processing practices. This proscribes unethical practices regarding individual users’ data such as unsolicited sales to third parties. In light of this principle, Home IoT manufacturers and processors would find it difficult to gather data under the guise of convenience and, consequently, to then conduct transactions with collected or aggregated personal data.

By establishing the above principles, the framers of the GDPR have recognized and have sought to address the perils associated with personal data collection. The GDPR acknowledges the existence of and rectifies the most prevalent security and privacy issues that could prejudice individual users. It actively shifts accountability to Home IoT manufacturers, as data controllers, and their corresponding data processors, but continues paving the way for misleading acts and subsequent thievery arising from unfairly drafted Terms and Conditions. Although the GDPR provides broad safeguards, the consent-based approach it establishes remains insufficient against contracts of adhesion. Admittedly, Terms and Conditions in the form of contracts of adhesion are, by far, the most practical way for Home IoT manufacturers and millions of individual users to enter into
contracts governing the use of Home IoT devices. However, there will always be instances when Home IoT manufacturers will ignore the law and brush aside accountability because potential profits far exceed any administrative fines they would face. This is not to say that lawmakers and regulators should establish stricter regulations or increase fines to deter this type of behavior. After all, too much regulation will effectively stifle innovation and inhibit any technological growth. Privacy and security breaches are best protected against not by regulation, but by vigilance. Additionally, the consent-based approach, and any regulation regarding privacy and security, will remain insufficient if individuals do not safeguard their personal privacy against breaches and unscrupulous practices.

B. The Sector-Based Privacy Protection Framework of U.S. and California Privacy Laws

Contrary to the EU’s overarching approach to data privacy and security through the implementation of the GDPR, the U.S. promotes a sector-specific approach through its “complex patchwork of state and federal privacy laws.”\(^\text{103}\) The fact that most of these laws are industry-specific means there is inadequate protection against and legal remedies for Home IoTs’ privacy violations.\(^\text{104}\)

The sector-specific approach is manifested in the absence of a single definition of “personal information” in the U.S. privacy protection framework. Rather, the definition is based on the “particular law that applies, the context in which it is used, and each organization’s privacy policies and procedures.”\(^\text{105}\) In this context, data collected and analyzed by Home IoT devices and their manufacturers is deemed personal data only if it is considered such under specific legislation.

In the absence of specific federal legislation, relevant principles and laws governing the protection of personal data arising from Home IoTs may include the Fair Information Practice Principles (FIPPS) and specific California laws such as the California Data Privacy Act of 2018 and the Shine the Light Law.

1. Fair Information Practice Principles (FIPPS)

FIPPS is a set of principles\(^\text{106}\) that serve as the cornerstone of federal and state privacy laws.\(^\text{107}\) It espouses privacy principles which serve as industry best practices and guides entities in collecting, using and protecting individual users’ personal information.\(^\text{108}\) It appears that Home IoT manufacturers are only encouraged, and not required, to adopt FIPPS in their organizational frameworks to protect their individual users’ privacy and to curtail any abuses arising from any unfair Terms and Conditions.\(^\text{109}\)

A number of the FIPPS principles are relevant in safeguarding against Home IoT manufacturers’ practice of drafting contracts in their favor, and consequently profiteering from any data “voluntarily” shared by individual users. Similar to the GDPR, FIPPS maintains the need to secure consent from individual users with regard to the “collection, use, dissemination, and maintenance” of their personal data, as manifested in the principle of Individual Participation.\(^\text{110}\) Apart from seeking consent from users, the FIPPS requires Home IoT manufacturers to bear responsibility for individual users’ personal data. The principle of transparency requires Home IoT manufacturers to inform users of the fact of “collection, use, dissemination, and maintenance” of personal data. In the same vein, the principle of purpose specification instructs Home IoT manufacturers to inform users of the purpose for which the data is collected; and the principle of data minimization limits collection to that which is “directly relevant and necessary to accomplish the specified purpose.” As espoused in the principle of use limitation, Home IoT manufacturers’ activity with regard to users’ personal data is limited to the specified purpose, and any sharing must be compatible with that purpose. Other principles include ensuring data quality and integrity, and establishing security over individual users’ personal data.

While establishing principles as a basis of federal and state privacy legislation is laudable, it remains inadequate as unscrupulous Home IoT manufacturers cannot be held liable under FIPPS for unfairly drafted Terms and Conditions in their favor. There is also no single piece of legislation which squarely governs Home IoTs, or IoTs in general, and proscribes against the misuses and abuses of personal data arising from obscure Terms and Conditions. Individual users and their personal data may be protected only if the misuse of data falls within a specific sector governed by relevant existing legislation.

2. California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 (Act) aims to protect individual consumers from data privacy abuses.\(^\text{111}\) Its scope focuses on California resident individuals “who [are] in the State for other than a temporary or transitory purpose, and [every individual] who [is] domiciled in the State [but] who is outside the State for a temporary or transitory purpose.”\(^\text{112}\) The Act equips individual consumers with the ability to request information as to the type and purpose of personal data that eligible for-profit entities collect from them.\(^\text{113}\) It likewise grants individual consumers a right to erasure but provides limitations
in cases of “completion of a transaction, research, free speech and some internal analytical use.” However, it remains to be seen whether the Act will sufficiently and effectively protect against the abuse of personal data of California resident individuals when it takes effect on January 1, 2020.

Although touted as the “strictest privacy bill in the history of the [U.S.],” it appears that the Act does not prohibit covered businesses from selling any personal data collected from individual consumers. As a safeguard, the Act recognizes a general opt-out approach to the sale of personal data, but specifically provides for an opt-in approach for certain minors. It requires covered businesses to post a “Do Not Sell My Personal Information” button on their online portals which individual consumers may click if they object to the sale of their personal data, and requires minors 16 and below to expressly opt-in to the sale of their data. Covered businesses are prohibited from discriminating against individual consumers who refuse to allow the sale of their personal data. However, these businesses may provide additional incentives to individual consumers who have disclosed more data.

Under the Act, Home IoT manufacturers may continue to sell personal data they have collected from individual consumers. They may even incentivize consumers to share more data. In this regard, it seems that the Act does not effectively protect individual consumers by failing to proscribe any unwarranted disclosure and sale. It continues to permit Home IoT manufacturers to hide behind Terms of Use to the detriment of the unsuspecting consumer.

3. California Shine the Light Law

More commonly known as the “Shine the Light” law, the clause on privacy rights in the California Civil Code grants California residents the right to know of any disclosures of their personal information by businesses for direct marketing purposes. Notably, the law limits the purpose to direct marketing and provides an exclusive list of personal information. The law discourages Home IoT manufacturers from disclosing individual users’ personal information to a certain extent. However, it fails to prevent manufacturers from unscrupulously gaining ownership of and profiting from other forms of data such as individual users’ preferences and daily habits. It likewise fails to protect against one-sided Terms and Conditions to the detriment of individual users.

In sum, the sector-specific privacy protection framework in the U.S. is lacking in protecting individual users’ privacy. Only sectors which have applicable legislation provide protection mechanisms. The absence of applicable law in a specific sector renders users open and defenseless against abuses of their privacy and personal data. More so, it could enable Home IoT manufacturers’ exploitation of users’ personal data by allowing them to hide behind seemingly fair Terms and Conditions.

V. CONCLUSION

The value of personal privacy is one of the foremost issues of the digital era. The convenience often associated with new technological developments has increasingly led to security and privacy risks. Home IoTs, in particular, have capitalized on individuals’ strong preference for convenience by providing easy solutions to everyday problems. However, individuals are barely aware that the use of Home IoT devices comes with the invisible price of loss of personal privacy.

Concerns about privacy protections have transitioned from how to reduce access to private information to how to maintain personal control over private information. The use of Home IoT devices encourages individuals to share personal data about their identities, preferences and daily habits. Unscrupulous Home IoT manufacturers, as data controllers, and their corresponding data processors, utilize one-sided and often arbitrary and obscure Terms and Conditions to acquire ownership and control over personal data collected. The seemingly innocuous act of skipping over lengthy Terms and Conditions may result in a transfer of rights over personal data. These contracts of adhesion promote unwarranted acquisition of data and deprive individual users of any opportunity to negotiate the contractual provisions, thus leaving them with no choice but to agree or their Home IoT devices will be rendered unusable.

The GDPR attempts to solve the security and privacy issues arising from one-sided Terms and Conditions. It requires Home IoT manufacturers to secure “freely given, specific, informed and unambiguous” consent based on Terms and Conditions written in “clear and plain language” and consistent with the principles of the lawful processing of data. The GDPR assigns accountability to Home IoT manufacturers and their corresponding processors. In effect, they are mandated to take responsibility to safeguard any data collected, transferred and analysed and prevent breaches arising therefrom. However, the consent-based approach mandated by the GDPR is not sufficient. It falls short of holding Home IoT manufacturers accountable for profiting from data. While the GDPR provides for substantial administrative fines in case of violations, many data controllers and processors feel they are above any means of regulation since they possess ample legal machinery to avoid penalties. In some cases, the monetary penalties are seemingly insubstantial compared to potential profits from commercialization of data.
Likewise, the U.S. sector-specific privacy protection framework is inadequate in protecting individual users’ privacy and personal data. Despite the overarching principles which in some cases effectively govern many sectors, the absence of relevant laws in other sectors allows for the exploitation of personal data, and continues to permit Home IoT manufacturers to utilize one-sided Terms and Conditions against unwitting individual users without any form of redress.

Under the current state of the law, the best way to protect against abuses is for individual users to take on this responsibility. As stakeholders, individual users need to understand their roles in the process of protecting their personal information. They need to be aware of the exposures involved in sharing personal data. Therefore, individual users should likewise bear the burden or the responsibility over their personal data and observe best practices in protecting their personal privacy. To promote individual users’ responsibility, it is vital to raise and increase awareness through education. Individual users should be made aware of their rights, security and privacy risks, the price of convenience as manifested in unscrupulous Terms and Conditions and most importantly the value of personal privacy. In the same vein, lawmakers should consider improving the current framework by exploring the feasibility of limited profiling and independent audits on data collection practices of Home IoT manufacturers to strive for ethical and fair undertakings throughout the industry. After all, full protection of privacy is best achieved through constant vigilance against unconscionable practices concerning personal data.

**ENDNOTES**


2. Id.


7. Thierer, supra note 5.

8. Id.


11. Posadas, supra note 6, at 75.


13. Id. at 819.


16. Id.


19. Thierer, supra note 5, at 8.


25. Meola, supra note 23.


* Celine Melanie A. Dee advises leading entrepreneurs and corporations on intellectual property, technology, and corporate law matters. Her research focuses on intellectual property and privacy protection in light of technology, innovation and development. She is expected to graduate from the University of Hong Kong in 2018, with Distinction, in the Master of Laws in Information Technology and Intellectual Property Laws program.
Adhesion: Contractual Clauses in a Transnational Electronic Contract of the Internet of Things We Don’t Own?

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

108 Sedona, supra note 106, at 291.


110 White House, supra note 108 (Individual Participation: Organizations should involve the individual in the process of using Personally identifiable information (PII) and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII).


112 Assemb. B. No. 375-1798.140 (g)

113 Id. 1798.100.

114 Id. 1798.125.


116 Assemb. B. 1798.135

117 Id. 1798.120 (d).

118 Id. 1798.125.

119 Id. 1798.125.


121 EDRi, supra note 3.
Mass incarceration in the U.S. today is a reality with global dimensions. With less than 5% of the world’s population, the U.S. houses 25% of the world’s known incarcerated population. In 2002, the United Nations Economic and Social Council adopted a resolution calling on member nations to draw upon the guidance of restorative justice programs and processes developed by a core group of experts, for the development of criminal justice reform. Since then, an increasing number of states in the U.S. have passed legislation that incorporates restorative justice as part of their criminal justice statutes, with some states merely approving the use of restorative justice and others actively promoting the implementation of restorative justice processes within their departments of corrections. This article discusses the problem of mass incarceration and highlights the need for an alternative approach to dealing with crime and deviance. Restorative justice is emerging as an increasingly viable approach for criminal justice systems around the world, as illustrated by examples in China and New Zealand. This article will discuss the basic concepts of restorative justice and the various ways in which restorative justice has been implemented in states such as Vermont. California’s recent adoption of restorative justice as part of its penal code in 2017 has provided a much-needed impetus for implementing restorative justice in this State. Restorative justice programs could be used for the rehabilitation and reentry into the community of large numbers of inmates who were transferred from prisons and held in county facilities, due to the passage of California’s Public Safety Realignment Act of 2011. Increasing public awareness and promotion of the understanding of restorative justice principles and practices will help us move towards a more humane and sustainable approach for dealing with crime and public safety.
incarceration is 114 prisoners per 100,000 residents, while Mexico’s rate of incarceration is about 164 prisoners per 100,000 residents.

Although public awareness is changing, and new sentencing policies and recent decreases in U.S. prison populations have reversed the upward trend in incarceration, some analysts note that the slow rate of decline in prison population could mean that it will take 88 years for the prison population to return to its 1980 level. Professor Michael Tonry of the University of Minnesota has pointed out that there has been no major legislation to unwind mass incarceration or rebuild U.S. sentencing systems, although the severity of repeat offender laws has been moderated, standards for parole release eligibility have broadened and prisoner reentry programs have been created and treatment programs expanded. No state has repealed a three-strikes law, life without parole, truth-in-sentencing law or created a broad-based mechanism for assessing the need for continued confinement of prisoners serving excessive sentences.

In 2010, Congress appropriated funds to the Bureau of Justice Assistance (BJA) to launch the Justice Reinvestment Initiative (JRI) in a public-private partnership with Pew Charitable Trusts (Pew) and other non-profit organizations to help states’ policy makers use data-driven approaches to curb correction spending, reduce recidivism and improve public safety. According to the June 2018 update from the Council of State Governments, so far 30 states have participated in JRI since 2010. JRI has been funded by a modest federal budget, starting at $10 million in 2010, peaking at $27.5 million in 2014-2017 and reducing slightly to $25 million in 2018. It has met with unqualified success achieving one of its main objectives of curbing prison or corrections spending. The Urban Institute reports that 28 states participating in JRI from 2010 to 2016 have reported more than $1.1 billion in savings and invested more than $446 million in criminal justice reform efforts.

Ironically, the truth-in-sentencing laws enacted by states in the 1990’s were propelled by federal funding for building additional prisons and jails authorized by Congress through the Violent Crime Control & Law Enforcement Act of 1994, buoyed by public sentiment for offenders to serve a large portion of their sentences. One of the key factors holding back the immediate repeal of such laws could be the high recidivism rate of former prisoners, based on a BJA Special Report published in 2014 on the pattern of recidivism of prisoners released in 2005 from 30 states over a five-year period from 2005 to 2010. Recognizing that decades-long upward spiraling spending on prison construction and harsh sentencing laws did not lower recidivism rates, the approach of JRI has been to provide support for participating states to invest in evidence-based policies and practices to promote rehabilitation of those incarcerated and improve public safety. The data and findings on the effects of the states’ shift towards justice reinvestment in community-based treatment and services, problem-solving courts, oversight councils and other reform measures are still being collected.

II. RESTORATIVE JUSTICE: INTRODUCTION

A. Comparing Restorative Justice with Retributive Justice

Some legal scholars have argued that change in our criminal justice system does not mean just change in sentencing practices, but also change in U.S. cultural traditions and public attitudes. In advocating for sentencing reform, Professor Tonry pointed out that the laws passed from 1984 through 1996 “attempted to remove compassion, empathy, and recognition of human weakness—something we all recognize in ourselves—from the processes by which punishments are imposed and administered.” Implementing sentencing reforms to reduce the prison population would not be sufficient to instill compassion and empathy in our criminal justice system. Adopting a restorative justice approach could provide this missing link.

Although restorative justice processes have been practiced in victim-offender mediation programs begun by Mennonite communities in Canada and the U.S. since the 1970’s, it was only in the 1990’s that there was an enormous growth in restorative justice programs around the world. Restorative justice has become increasingly popular in response to the harsh and highly impersonal type of retributive justice meted out against criminal offenders. Howard Zehr, a leading proponent of restorative justice, explains that restorative justice involves a shift in worldview that focuses on crime as “a violation of people and relationships,” necessitating the administration of justice involve the search for solutions promoting the repair of community relations, reconciliation and reassurance. Thus, a restorative justice model would more easily incorporate rehabilitation programs and processes for reintegration of prior offenders into society.

Restorative justice is a community-based concept of justice. Many restorative justice initiatives are based on volunteerism and significant numbers of community members participate in their operation. Restorative justice practitioners such as attorney Marina Sideris, who serves on the Restorative Justice Institute of Maine, consider restorative justice to be a locally-based practice. Ms. Sideris cites both her state and the federal Bill of Rights which provide that a criminal trial is before “an impartial jury of the state and district wherein the crime shall have been committed,” as supporting the notion that criminal
justice involves inherently local processes. Specifically, when a crime is committed, then discretionary local actors make choices, such as the local police who decide how to respond and whether to charge the offender, local prosecutors who decide whether to prosecute and what the proper punishment should be and local jurors who decide what constitutes proof beyond a reasonable doubt. Those who are experienced in restorative justice practice believe that the strength and efficacy of restorative justice programs depend on the strength and engagement of the local community, more akin to a voluntary grass-roots movement. This is another major difference between restorative justice processes and formalistic retributive justice institutions.

Some legal scholars have expressed reservations that the restorative justice approach does not yield uniformity in outcomes among similarly-situated cases. While restorative justice proponents want participants in restorative justice processes to decide upon a resolution of their particular issue or circumstances, retributive theorists and traditional lawyers want to impose external constraints to achieve uniformity of outcomes. For example, Professor Tonry has argued that the result of similarly situated offenders who have committed comparable offenses receiving different negotiated penalties through a restorative justice process, would be unjust. However, the retributive justice approach does not result in uniformity of outcomes in practice either. For instance, all the lofty theorizing about uniformity in sentencing makes little difference to a poor or marginalized defendant who has to accept a false plea bargain because he or she cannot make bail. How is the outcome uniform when a rich defendant can afford the legal fees of a high-priced defense team for dismissing criminal charges based on a technicality? There are valuable social benefits (some would consider it an immeasurable value) when a former offender learns empathy and accountability for dismissing criminal charges based on a technicality? There are valuable social benefits (some would consider it an immeasurable value) when a former offender learns empathy and accountability through a restorative justice program and is able to move on to a life as part of his or her community.

B. Restorative Justice in a Multi-Racial and Pluralistic Society

Concerns have been raised about the potential for racially disparate impacts of restorative justice programs in a multi-racial society. For example, some writers have worried that courts will not be inclined to divert poor, minority youths to neighborhood-based restorative justice programs at the same rate as they do for middle class youths coming from more established communities. Others seem to think that the success of restorative justice programs (which require substantial citizenship participation and correctional policies which support such volunteer participation) in places like Vermont would not be easily replicated in communities which are more diverse. A leading expert on restorative justice and human rights, Professor Theo Gavrielides, noted that the hope that restorative justice would provide a better experience of justice for those who are let down the most by the criminal justice system, would not be realized if we do not address the power structures inherent in our current framework of criminal justice. Studies in critical race theory teach us that criminal justice institutions and systems perpetuate the racial hierarchy and inequality in society. Since restorative justice programs are being espoused as a response to the failures of our current criminal justice system, policy makers and researchers have been urged to implement pilot studies and develop restorative justice programs or processes that address race relations and the impact on communities of color. For example, restorative justice practices can be developed which “support individuals and communities during racial conflicts by creating conditions for mutual understanding and collaborative action rather than by seeking to exclude or punish.”

C. The Need for Public Support for Restorative Justice in the U.S.

Previously, public support for tough sentencing policies rose sharply in the U.S. in the 1970’s and remained high until the late 1990’s. Due to the widely perceived problems of mass incarceration and criminal justice failures such as racial disparities, wrongful convictions and high recidivism rates, there is significant public opposition to retributive sentencing and zero-tolerance policies and growing public support for criminal justice reform. Despite the softening of public attitudes towards crime over the past two decades, as shown by public opinion surveys, the incarcerated population in the U.S. has only dipped slightly below its all-time high.

Recent public opinion surveys conducted from 2012 to 2015 by Marquette Law School in Wisconsin have shown significant gaps and variance in public perceptions about how well the criminal justice system performs and what the criminal justice system should prioritize, depending on the social group, race and political party affiliation of those being surveyed. For instance, skepticism towards rehabilitation appeared to be influenced by racial attitudes and political ideology. The researchers noted that different segments of the public existed in different worlds of criminal justice, with diverging perceptions and differing sources of information. One inference drawn by the researchers of the Marquette Law School survey was that the racial attitudes of some members of the public towards rehabilitation programs as a type of affirmative action program could explain why policy makers were ambivalent towards supporting rehabilitation programs and why there was chronic underfunding of rehabilitation programs in this country. Another recent study regarding the future of
restorative justice in criminal justice reform measures in the U.S. has also confirmed the “mismatch between perceived support for [restorative justice] and actual support in terms of funding for implementation.” The challenge of under-funding seems to be a major obstacle facing the implementation of restorative justice programs and practices in this country. Therefore, one of the tasks facing proponents of restorative justice is to promote public awareness and support for restorative justice.

III. PRINCIPLES AND PRACTICES OF RESTORATIVE JUSTICE: A GLOBAL PERSPECTIVE

A. U.N. Guidance on Restorative Justice

In August 2002, the United Nations Economic and Social Council adopted a resolution calling upon member states implementing restorative justice programs to draw on a set of “Basic Principles on the Use of Restorative Justice Programmes in Criminal Matters” (Basic Principles). The Basic Principles offer guidance for policy makers, community organizations and criminal justice officials involved in the development of restorative justice responses to crime in their society. The preamble to the Basic Principles notes that restorative justice gives rise to a range of measures that are flexible in their adaptation to established criminal justice systems and that complement those systems, taking into account legal, social and cultural circumstances. An illustrative diagram of different ways that restorative justice processes can be implemented is reproduced in Diagram 2, below.

The Basic Principles provide guidance on the operation of restorative justice programs, stating that member states should establish guidelines and standards, with legislative authority when necessary, that govern the use of restorative justice programs. Guidelines for restorative justice programs should address:

1. the conditions for the referral of cases to restorative justice programs;
2. the handling of cases following a restorative process;
3. the qualifications, training and assessment of facilitators;
4. the administration of restorative justice programs; and
5. standards of competence and rules of conduct governing the operation of restorative justice programs.

In addition, procedural safeguards should be developed to guarantee fairness to the offender and the victim, such as:

1. subject to national law, the victim and offender should have the right to consult with legal counsel concerning the restorative process and, where necessary, to translation and/or interpretation. Minors should, in addition, have the right to the assistance of a parent or guardian;
2. the parties should be fully informed of their rights, the nature of the process and the possible consequences of their decision; and
3. neither the victim nor the offender should be coerced, or induced by unfair means, to participate in restorative processes or to accept restorative outcomes.

The results of agreements arising out of restorative justice programs should, where appropriate, be judicially supervised or incorporated into judicial decisions or judgments. Where that occurs, the outcome should have the same status as any other judicial decision or judgment and should preclude prosecution based on the same facts. Where no agreement is reached among the parties, the case should be referred back to the established criminal justice process and a decision as to how to proceed should...
be taken without delay. Failure to reach an agreement alone shall not be used in subsequent criminal justice proceedings.

As shown in Diagram 2 above, a referral to a restorative justice program can be initiated at various points: (1) at the police level (pre-charge); (2) at the prosecution level (post-charge but usually before a trial); (3) at the court level (either at the pre-trial or sentencing stage); and (4) at the corrections level (as an alternative to incarceration or as part of a non-custodial sentence). At any one of these points, there is an opportunity for officials to use their discretionary authority to refer an offender to a restorative justice program. Restorative justice processes can also be implemented during incarceration or after release from prison.

B. Restorative Justice Practices in the International Community

Restorative justice has become a worldwide criminal justice reform movement with close to 100 countries using restorative practices in addressing crime. In China, restorative justice theory started to be disseminated in academic circles and publications in 2002, although China already had a long tradition of mediation. In his survey of restorative practices in Asia, Professor John Braithwaite noted that there were about 155,000 local mediation committees in China in the 1990’s, which handled over 6,000,000 cases, while under 4,000,000 cases went to court. A research study on community justice institutions in China focused on bang jiao meetings (bang means “help” and jiao means “education” and “admonition”). The bang jiao meetings tend to start as stigmatizing encounters but end as reintegrative encounters for the offender.

One case example involved a 27-year-old young man who killed his own father out of rage at seeing his father beating his mother very badly. He was sentenced to prison for eight years. Due to his good performance in the labor camp, he was released after serving a five-year sentence. But his family members did not forgive him. Bang jiao team members realized that it was a difficult situation because of mixed feelings about the young man in an already crowded household. They made frequent visits to the home and tried to persuade the family to forgive and accept the young man. However, after only two weeks of his release, he was caught stealing at the local store. When the bang jiao team members arrived at the local police station, they soon realized that he stole because his family members did not give him living necessities. Bang jiao members persuaded local police to drop the charges. A month later, they arranged a job for him at the community-run factory. He saved money from his salary to buy fruits and nutritious products for his grandmother. He spent hours taking care of his sister-in-law during her pregnancy. After the birth of her baby daughter, he took care of all three generations because his brother worked long hours as a truck driver. After two agonizing years, the family members were moved by the young man’s sincerity and accepted him back. The young man honored the bang jiao members who helped him, saying that he would probably have committed suicide without them.

New Zealand is another country which implemented restorative justice on a national scale. Its ministry of justice followed the U.N. guidance on restorative justice principles in its 2004 publication on “Principles of Best Practice for Restorative Justice Processes in Criminal Cases” based on a consultative process with restorative justice practitioners. Acknowledging that there is no universal definition of restorative justice, it has described restorative justice as “a process to involve, to the extent possible, those who have a stake in a specific offense and to collectively identify and address harms, needs and obligations, in order to heal and put things as right as possible.” In New Zealand, restorative justice practices resonated with the traditional values of reconciliation, reciprocity and community (“whanau”) involvement emphasized in the social practices of the indigenous Māori culture. The country started applying restorative justice principles and practices with its introduction of a family group conference (i.e., a type of restorative justice process) for young offenders in 1989. In 2002, restorative justice processes were first enacted into its criminal justice statutes through passage of the Sentencing Act 2002, Parole Act 2002 and Victims’ Rights Act 2002. Although the U.N. model (as illustrated by Diagram 2 above) shows that restorative justice processes can be implemented at different stages of the criminal justice system, the most common restorative justice processes in New Zealand are the pre-sentencing referrals from the district court and the Police Adult Diversion Scheme to restorative justice programs.

The New Zealand Ministry of Justice has published reports on the rate of re-offending among offenders who participated in restorative justice programs. For example, the ministry published a 2014 report based on statistical studies of 2,323 offenders referred to restorative justice programs during the period 2008 to 2011, comparing them to 6,718 offenders who were not referred to a restorative justice program. One of the findings of the report is that offenders who participated in a police-referred or court-referred restorative justice conference committed 23% fewer offenses during the subsequent 12-month period than comparable offenders who did not participate in restorative justice conferences. Another finding is that offenders who participated in a police-referred or court-
referred restorative justice conference had a 12% lower rate of reoffending during the subsequent 12-month period than comparable offenders who did not participate in restorative justice conferences.

IV. IMPLEMENTATION OF RESTORATIVE JUSTICE IN THE US

A. Restorative Justice in Practice

According to a 2016 Pew report, there are 35 states in the US with some form of restorative justice statute in place, although some states merely define the practice of restorative justice while others promote its use in public agencies or corrections. Vermont and Colorado have passed laws that encourage the use of restorative justice on a statewide basis, and have created agencies that oversee or provide the service. Restorative justice programs are currently being implemented in a variety of ways by different states.

Although in many states in the U.S. offenders serving time are barred from contacting victims, some states have started victim-offender dialogue programs for inmates. Texas has one of the largest victim-offender dialogue programs in the country, but the focus is entirely on the victim rather than rehabilitating the offender. It must be the victim who initiates the process and each victim has his or her own reasons for doing so. Setting up a dialogue takes months of work. Program staff meet with both sides separately to prepare them for the encounter. In Texas, participation is voluntary for inmates and is confidential, which means prisoners cannot bring up their participation before the parole board. In Massachusetts, the restorative justice program run by the Department of Corrections allows for volunteer participation but does not include victims in the dialogue sessions. According to a criminal justice professor who offers an eight-week course on restorative justice at a prison in Norfolk, Massachusetts, the inmates gain empathy when a survivor (not the actual victim) shares the trauma that she or he experienced.

Other states such as Vermont are using restorative justice to help offenders re-enter society. In 2006, Vermont started hosting “circles of support and accountability” in its community justice centers for high-risk offenders who had committed serious crimes (such as sexual assault and domestic violence) to help with re-entry. Recently released inmates are matched with three to four volunteers from the community to participate in a circle conference where they can talk about the choices that landed them in prison as well as thinking patterns and returning to the community. These community justice centers host about 60 circles per week and each circle costs about $10,000 per year for the state. A 2014 study found that 27% of offenders who participated in the circles were convicted of new crimes, compared with 44% for non-participants.

On a less formal level, restorative justice programs operated by non-profit organizations have sprung up throughout the country and provided mediation services for many years, with the cooperation of local law enforcement, without any official recognition by the state. A national survey published in 2000 by the U.S. Department of Justice, Office for Victims of Crime, identified about 289 victim-offender mediation (VOM) programs offered in the U.S. in 1996. About 43% of the VOM programs were sponsored by private community-based agencies, 22% were sponsored by church-based organizations, 16% were sponsored by probation departments, 8% were sponsored by correctional facilities, 4% were sponsored by prosecutors’ offices, 3% were sponsored by victim services agencies, 2% were sponsored by police departments and 2% were sponsored by residential facilities. There has been no other comprehensive survey published by the U.S. Department of Justice on restorative justice organizations and funding since the above survey was published in 2000. A recent article by sociologists David Karp and Olivia Frank reported that the median funding for 56 restorative justice non-profit organizations surveyed from 2003 to 2013 had increased five-fold from $26,039 per year to $122,235 per year. However, they pointed out that a non-profit organization with $120,000 in annual funding can barely pay for a small office with one or two staff members.

B. California’s Shift Toward Restorative Justice

Effective January 1, 2017, Penal Code section 1170 in California has been amended to state, in pertinent part, as follows:

(a)(1) The Legislature finds and declares that the purpose of sentencing is public safety achieved through punishment, rehabilitation, and restorative justice. When a sentence includes incarceration, this purpose is best served by terms that are proportionate to the seriousness of the offense with the provision for uniformity in the sentences of offenders committing the same offense under similar circumstances. (2) The Legislature further finds that programs should be available for inmates, including but not limited to, educational, rehabilitative, and restorative justice programs that are designed to promote behavior change and to prepare all eligible offenders for successful reentry into the community.
This is a deep-sea change from the prior legislative declaration on the purpose of sentencing in California, which stated in former Penal Code section 1170 that:

(a)(1) The Legislature finds and declares that the purpose of imprisonment for crime is punishment. This purpose is best served by terms proportionate to the seriousness of the offense with provision for uniformity in the sentences of offenders committing the same offense under similar circumstances. The Legislature further finds and declares that the elimination of disparity and the provision of uniformity of sentences can best be achieved by determinate sentences fixed by statute in proportion to the seriousness of the offense as determined by the Legislature to be imposed by the court with specified discretion. (2) Notwithstanding paragraph (1), the Legislature further finds and declares that programs should be available for inmates, including but not limited to, educational programs, that are designed to prepare nonviolent felony offenders for successful reentry into the community.

According to the author of Assembly Bill 2590 (AB 2590), California’s criminal justice system, previously founded on the sole purpose of punishment, has failed, and despite overcrowded prisons, recidivism remained at the unacceptably high rate of 61%. The prior legislative declaration of punishment as the primary purpose of sentencing was first enacted in 1977, through California’s Uniform Determinate Sentencing Act, based on punitive models of criminal justice advocated in the 1970’s. The impetus behind AB 2590, signed into law by the California Governor on September 27, 2016, known as the Restorative Justice Act, was to stabilize the advances made by California in reducing its prison population pursuant to the ruling of the U.S. Supreme Court in Brown v. Plata, 1310 U.S. 1910 (2011). The Supreme Court mandated that California prisons reduce their overcrowded conditions that resulted in suffering and deaths of inmates in violation of the Eighth Amendment prohibition against cruel and unusual punishment. Much of the decrease in the U.S. prison population from 2009 to 2014 was attributed to the Plata decision which required California to release 35,000 prisoners to remedy prison overcrowding.

In response to the Plata ruling, California passed the Public Safety Realignment Act in 2011 to reduce prison overcrowding. However, observers have postulated that the Realignment Act merely moved prison inmates to county jails without really reducing California’s overall incarceration rate. According to Professor Joan Petersilia of Stanford Criminal Justice Center, this shift in custodial responsibility to county agencies could be a positive development if it could facilitate the delivery of locally-based treatment programs and reentry plans that will connect newly released inmates to jobs, families and support systems.

According to the California Legislative Analyst’s Office, it costs about $70,812 per year to incarcerate an inmate in California in 2016-2017. The average annual cost has increased by about $22,000 per prisoner, or 45%, since 2010-2011, during the period when the Plata ruling was issued on May 23, 2011. According to a report by the Vera Institute of Justice, California previously held the most prisoners in 2010, at 168,044 prisoners, but has reduced them by 21% in 2015, to 132,992 prisoners, being surpassed only by Texas as the state with the most prisoners at 149,159 prisoners. However, California’s prison expenditures in 2015 were still the highest at $8.6 billion (a 7% increase from 2010), followed by New York at $3.69 billion and Texas at $3.28 billion.

California would do well to follow the example of Hawai’i where restorative justice has been a mandated component of its reentry system since 2007. Compared with California’s incarceration costs of $64,642 per inmate in 2015, Hawai’i’s prison expenditures were $29,425 per inmate in 2015.

Adopting measures to reduce recidivism among former inmates not only promotes social reintegration and supports public safety, it also saves taxpayer money in the long run. Introducing bold initiatives, increasing public awareness and promoting the growth of restorative justice programs at the grass-roots level would be necessary steps for true and lasting reform.

V. THE ROLE OF RESTORATIVE JUSTICE FOR THE FUTURE OF OUR COMMUNITIES

In this age of mass incarceration, the values and processes of restorative justice are badly needed to restore and heal communities adversely impacted by the punitive policies of the War on Drugs and the War on Crime which disproportionately impacted marginalized communities and communities of color. The account provided by a former inmate, Herb Blake, who participated in restorative justice through victim-offender dialogue sessions held during his incarceration, tells us that restorative justice is another name for empathy and compassion. In his words, “Restorative justice is not just for law breakers. It is a model by which we can heal our community. Our community needs a lot of healing—children are put in prison for life; women are sent to prison for defending themselves against abuse; and the elderly are sent to prison to die.” He tells us of a 72-year old man he met in prison, arrested for a crime that would ordinarily carry a maximum two-year sentence, but who was on his eighth year of a 25 year-to-life sentence under the three-strikes law, due to an old assault conviction from 1957.
and a drug conviction from the 1970’s. As Mr. Blake puts it, due to the impact of mass incarceration, “we are breeding a subculture of bitterness and enmity.” He points out that men and women need community support when they are released from prison but the response has been far less than what is needed to accommodate the recently-released population.

Renata Valree, the current Chair of the Board of Directors for the National Association for Community Mediation, has played a key role in developing restorative justice programs throughout the U.S. She notes that some factors to be taken consideration when developing a restorative justice program include: (1) how is justice perceived in the community; (2) what needs are unmet that restorative justice could help to fill; (3) coalition building—identifying and working with other groups which provide services related to public safety and justice; (4) public awareness and education by hosting listening sessions and/or community forums; and (5) whether the restorative justice program should be community-based (e.g., using a community mediation center) or system-based (i.e., affiliated with the criminal justice system). According to Ms. Valree, restorative justice helps former offenders move past punishment, restore a sense of connection to their community and transforms them by helping them grow into law-abiding citizens.

In his widely viewed TED Talk in 2012, human rights lawyer Bryan Stevenson shares with the audience what he learned from his work in representing death row inmates. In his words, “[i]t’s just taught me very simple things. I’ve come to understand and to believe that each of us is more than the worst thing we’ve ever done. … if somebody tells a lie, they’re not just a liar … if somebody takes something that doesn’t belong to them, they’re not just a thief … even if you kill someone, you’re not just a killer.” Professor Stevenson, who teaches at New York University School of Law, informs us that in Alabama where a criminal conviction will result in permanent disenfranchisement, about 34% of the black male population has lost the right to vote. He also reminds us of the fact that in the states of the old South, a defendant is 11 times more likely to get the death penalty if the victim is white than if the victim is black, and 22 times more likely to get the death penalty if the defendant is black and the victim is white. As stated by Professor Stevenson, our identity is at risk. … Despite the fact that it is so dramatic and so beautiful and so inspiring and so stimulating, we will ultimately not be judged by our technology, we won’t be judged by our design, we won’t be judged by our intellect and reason. Ultimately, you judge the character of a society, not by how they treat their rich and the powerful and the privileged, but by how they treat the poor, the condemned and incarcerated.

As we face new frontiers as a nation, we also risk bringing our present-day realities of suffering, abuse, degradation and marginalization with us. Hopefully, our communities will have implemented restorative justice solutions and ended mass incarceration before we reach the next human frontier.

ENDNOTES

4 See World Prison Brief, supra note 3.
5 Marc Mauer & Nazgol Ghandnoosh, Can We Wait 88 Years to End Mass Incarceration?, HUFFINGTON POST, Dec. 20, 2013 (noting that the prison population declined by 1.8 percent between 2011 and 2012).
7 Id.
8 See Samantha Harvell, et. al., Reform Sentencing & Corrections Policy: the Experience of Justice Reinvestment Initiative States (URBan Inst. 2016). JRI collaborators include: BJA (which funds and oversees the JRI), Pew (which funds and supports JRI through education & research), Vera Institute of Justice and Council for State Governments (which provides technical assistance for states participating in JRI) and Urban Institute (which assesses the impact of JRI).
10 Harvell et. al., supra note 8, at 70-71.

* Jennifer Lim is an attorney practicing immigration and naturalization law in Los Angeles, California. She has represented defendants in post-conviction relief before California’s criminal courts, and currently serves on the steering committee of the Crossroads Restorative Justice Project in Compton, California.
bjs.gov/content/pub/pdfs/tssp.pdf (Sept. 10, 1998) (reporting on page 3 that to qualify for such federal grants, states must require individuals convicted of a Part 1 violent crime to serve not less than 85% of their prison sentence).

12 Bureau of Just. Assistance, Recidivism of Prisoners Released in 30 States in 2005: Patterns from 2003 to 2010, 2014, doc. no. NCJ 244205, https://www.bjs.gov/content/pub/pdf/rprtd05p0510.pdf (last visited Sept. 10, 2018) (reporting on page 7 that 43.4% of those released were arrested within the first year of release from prison which increased to 76.6% of those released by the end of five years. The longer that released prisoners went without being arrested, the less likely they were to be arrested within the five-year period; see Table 16 on page 15 for the data on being incarcerated for a new crime over the five-year period after release).


14 Harvell, et al., supra note 8, at 34 (stating that it is too early in some states to track progress even at the system level).


16 Tonry, supra note 6, at 444.


18 Hill, supra note 17, at 118; see also John Braithwaite, Principles of Restorative Justice, Restorative Just. and Crim. Just. (Andrew Von Hirsch, Julian Roberts, Anthony Bottoms eds. (2003)).


21 Id. at 151 n. 1 (citing Me. Const., art. 1, § 6; U.S. Const. amend. VI).

22 Id. at 149 (discussing the history of the restorative justice movement in Maine, which had strong beginnings in the late 1990’s but the state’s original restorative justice statute faced repeal in 2007 when pilot projects throughout the state were closed).


24 Id. at 1269-70.


29 See Gavrielides, supra note 27, at 231.

30 Mark Ramirez, Punitive Sentiment, Criminology, vol. 51 (2013), at 337.


33 Id. at 50-51.

34 See Karp & Frank, supra note 31, at 13 (this study was conducted by sociologists using interviews of academics and practitioners of restorative justice, research and media databases and database searches of non-profit organizations and their funding).


36 Id. at 14.

37 Id.


41 Id. at 6.

42 Id. at 7.


44 Rebecca Beitsch, Victims and Offenders Come Together to Make their Own Justice, Stateline 2-3 (July 20, 2016).

45 Id.


47 Id.

48 Id.

49 Id.

Id.

See Karp & Frank, supra note 31, at 14.

See Notes of the Senate Committee on Public Safety Hearing Held on June 28, 2016, on Asemb. B. 2590.

See Ruth Gilmore, *Golden Gulag: Prisons, Surplus, Crisis and Opposition in Globalizing California* 89 (2007) (legislative declaration of 1977 ended the state’s prior sixty-year history in using its prison system as a means of rehabilitation for all but the most intransigent and incorrigible, and on pages 5-7, discussing the growth of the California prison system which grew almost 500% between 1982 to 2000 and built twenty-three new major prisons between 1984 to 2007). See also James Q. Wilson, *Thinking about Crime* 254 (1975) (advocating for a punitive model of criminal justice, higher imprisonment rates and no further spending on rehabilitation measures).

*Tony*, supra note 6, at 443 (citing Joan Petersila, *California Prison Downsizing and its Impact on Local Criminal Justice Systems*, Harv. L. and Pol’y Rev. 8:327 (2014)).

*See Petersila*, supra note 55, at 350-57.


*See https://www.nafcm.org/page/PeopleCurrent*? (last visited on July 12, 2018). During her tenure as Program Director of the Dispute Resolution Program of the Office of the City Attorney of Los Angeles, Ms. Valree helped design the Neighborhood Justice Program which allowed first-time, non-violent offenders to appear before a panel of community volunteers to discuss the crime and its harm to the victims and community, instead of going to court. (Information on restorative justice programming from Ms. Renata in this article is based on a telephonic interview conducted by the author on July 12, 2018.)

*See Phillip Meyer, Storytelling: Attorney Bryan Stevenson Tells Stories to Change the Shape of the World*, ABA J. 22-23 (May 2018); see also *Bryan Stevenson, Just Mercy* (2014), a biographical account of Prof. Stevenson’s work through Equal Justice Initiative in defending death row inmates in the South.

*See https://www.ted.com/talks/bryan_stevenson_we_need_to_talk_about_an_injustice.*

Id.

---

**Join us for ILS’s Careers in International Law Program!**

**FEBRUARY 4, 2019**

**12:00 pm – 1 pm**

University of California, Irvine School of Law

Education Building, Room EDU 1111

This panel discussion will be led by speakers William Gay, Margrette Francisco, Juan Zuniga and Agustin Ceballos, all of whom have a broad range of experience as to international law—ranging from cross-border transactions to global compliance. The discussion will focus on different career paths in international law and how to pursue them.

Please contact Tiffany Heah if you plan to attend at ils@calawyers.org.
I. INTRODUCTION

The Trump Administration has taken dramatic steps and made some significant decisions in the area of international trade, in particular on aluminum and steel tariffs. This article will explore certain of the Administration’s recent trade-related decisions under the Trade Expansion Act of 1962 and the possible legal ramifications for California practitioners.

The article surveys the Trade Expansion Act and highlights its historical application by various Presidents. It then explores the reaction of key U.S. trading partners to the recent steel and aluminum measures, including claims rooted in World Trade Organization (WTO) commitments and jurisprudence. It closes with observations about the role that the WTO may play in future trade actions. In short, this article aspires to be a timely resource for California practitioners working to advance their clients’ interests in a time of change.

II. ACTIONS BY THE TRUMP ADMINISTRATION

On April 20, 2017, President Donald J. Trump issued a Presidential Memorandum in which he directed the Secretary of Commerce to review whether the importation of certain steel mill products into the U.S. posed a threat to the national security of the U.S. On April 27, 2017, the President issued a parallel Presidential Memorandum directing a similar review of the importation of certain aluminum products into the U.S. For reasons that will be discussed, responsibility for these reviews fell to the Bureau of Industry and Security within the Department of Commerce (BIS). The legal ground cited for these investigations was a peculiar federal statute, the Trade Expansion Act of 1962 (Act), specifically Section 232 of the Act.

The BIS subsequently issued its reports on steel and aluminum dated, respectively, January 11, 2018 and January 17, 2018. For steel, the BIS found, *inter alia,* that:

1. steel is important to the national security of the U.S.;
2. imports of steel in such quantities as presently found adversely impact the economic welfare of the U.S. steel industry;
3. displacement of domestic steel by excessive quantities of imports has the serious effect of weakening the internal economy of the U.S.; and
4. a global excess in steel capacity is a circumstance that contributes to the weakening of the U.S. economy.

In its aluminum report, the BIS found, *inter alia,* that:

1. aluminum is essential to the national security of the U.S.;
2. the U.S. Government does not maintain strategic stockpiles of bauxite, alumina, aluminum ingots, billets or any semi-finished aluminum products such as aluminum plate;
3. the present quantity of imports adversely impacts the economic welfare of the U.S. aluminum industry; and
4. a global excess of aluminum capacity is a circumstance that contributes to the weakening of the U.S. industry and the U.S. economy.

On March 8, 2018, President Trump issued a Presidential Proclamation in which he ordered the imposition of a 25% *ad valorem* tariff on certain steel articles and a 10% *ad valorem* tariff on certain aluminum articles. On May 31, 2018, President Trump issued a Presidential Proclamation imposing the steel tariffs on steel imported from all countries except Australia (which is exempt) and three countries subject to annual quotas (South Korea, Argentina and Brazil). On the same date, President Trump issued a Presidential Proclamation imposing the aluminum tariffs on aluminum imported from all countries except Australia (which is exempt) as well as Argentina (which is subject to an annual quota). These steel and aluminum tariffs became effective on June 1, 2018.
In a subsequent move that received less attention than the steel and aluminum investigations, on May 23, 2018, the Department of Commerce announced that it was undertaking a Section 232 investigation into whether imports of automobiles (including SUVs, vans and light trucks) and automotive parts into the U.S. threaten the national security of the U.S. as defined in Section 232 of the Trade Expansion Act of 1962.11

III. GOVERNMENT POWER TO EXECUTE TRADE POLICY

Constitutional and other legal questions about respective federal authorities to design and execute U.S. international trade policies enjoy a rich history. Article II, Section 2 of the U.S. Constitution confers upon the President the power to make treaties and to function as the Commander in Chief while Article I, Section 8 confers upon Congress the power to regulate commerce with foreign nations and to lay and collect taxes and duties.12 The allocation of authority to these two branches of government is a robust example of the concept of separation of powers.

Given their crucial role in trade relations between states, tariffs and other import impediments have frequently been the venue of constitutional and legal questions. At the same time, tariffs have also been the impetus for pragmatic decisions between the executive and legislative branches. For example, the Reciprocal Trade Agreement Act of 1934 effectively functioned as a delegation of Congressional authority to the President to negotiate tariff reductions with U.S. trading partners.13 Although an acknowledgement that Congress lacked the constitutional standing—let alone the practical ability—to negotiate tariff reductions, this delegation proved to be unsatisfactory to Congress and in 1948 it refused further extensions of the Reciprocal Trade Agreements Act. This, however, was not before Presidents Roosevelt and Truman used it as a legal authority on the basis of which they negotiated tariff reductions with key trading partners. These, in turn, played no small part in laying the foundation for the launching of the General Agreement on Tariffs and Trade in 1948 (the precursor to today’s WTO). This example confirms an early precedent that Congress can and does delegate its authorities on tariff matters to the President.

Indeed, the Act was (and is) such a delegation of authorities to the President. President John F. Kennedy signed the Act on October 11, 1962, and commented upon doing so that:

This act recognizes, fully and completely, that we cannot protect our economy by stagnating behind tariff walls, but that the best protection possible is a mutual lowering of tariff barriers among friendly nations so that all may benefit from a free flow of goods. Increased economic activity resulting from increased trade will provide more job opportunities for our workers.14

It is important to underscore that the Trade Expansion Act was regarded by both Congress and President Kennedy as a delegation of Congressional authority to the President to negotiate tariff reductions with trading partners. But whereas the text and legislative history of the Act point to the overall mission of reducing tariffs, the Act also provided for various exceptions to this charge. National security is one such exception, codified in Section 232 (under the subtitle “Prohibition on decrease or elimination of duties or other import restrictions if such reduction or elimination would threaten to impair national security”) as follows:

No action shall be taken pursuant to section 1821(a) of this title or pursuant to section 1351 of this title to decrease or eliminate the duty or other import restrictions on any article if the President determines that such reduction or elimination would threaten to impair the national security.15

By way of explanation, 19 U.S.C. § 1821(a) empowers the President to enter into trade agreements to address duties or import restrictions when the President “determines that any existing duties or other import restrictions … are unduly burdening and restricting the foreign trade of the United States.”16 Similarly, under this authority the President may also “proclaim such modification or continuance of any existing duty or other import restriction, such continuance of existing duty-free or excise treatment, or such additional import restrictions, as he determines to be required or appropriate to carry out any such trade agreement.”17

Initially found in the Reciprocal Trade Agreement Act of 1934 (see supra), 19 U.S.C. § 1351 articulates when the President may enter into foreign trade agreements, or modify/continue existing duties or import restrictions, “for the purpose of expanding foreign markets for the products of the United States (as a means of assisting in establishing and maintaining a better relationship and maintaining a better relationship among various branches of American agriculture, industry, mining, and commerce).”18 Providing the pivotal linkage between the expansion of foreign markets and imports into the United States, Congress further provided that the President may pursue that purpose:
by regulating the admission of foreign goods in the United States in accordance with the characteristics and needs of various branches of American production so that foreign markets will be made available to those branches of American production which require and are capable of developing such outlets by affording corresponding market opportunities for foreign products in the United States.19

This provision articulates the manner in which a statute designed to open foreign markets to U.S. exports transitions into a basis for restricting imports into the U.S. as a means of leverage. Though not explicit, there is a sense of proportionality and reciprocity (if not forced) in the above statutory authority.

When the President finds “as a fact that any existing duties or other import restrictions of the United States or any foreign country are unduly burdening and restricting the foreign trade of the United States,” the President is authorized to:

(a) enter into foreign trade agreements with foreign governments or instrumentalities thereof and, (b) to proclaim such modifications of existing duties and other import restrictions, or such additional import restrictions, or such continuance, and for such minimum periods, of existing customs or excise treatment of any article covered by foreign trade agreements, as are required or appropriate to carry out any foreign trade agreement that the President has entered into hereunder.20

This is the core statutory foundation upon which the Trump Administration rests its current Section 232 actions involving steel and aluminum. It is noteworthy that neither the steel nor the aluminum reports from the BIS in 2018 claim direct legal foundation on any statutory grounds other than the Trade Expansion Act of 1962.21

IV. LEGAL CHALLENGES TO SECTION 232

The tension between the legislative history lying behind the Act and the manner in which the Act has been utilized by various Presidents is relevant to international trade governance and domestic legal challenges. While no administration has launched the number of Section 232 investigations in its first months as the Trump Administration has, there is precedent for such investigations. There are fewer precedents, however, for such investigations leading to the imposition of import restraints.

Since it assumed administrative responsibilities for such investigations in 1980, the Department of Commerce undertook 16 formal investigations of the national security impact of imports under Section 232 before the recent steel and aluminum investigations launched in 2017.22 These investigations and the resulting presidential actions are set out in the following table:23

<table>
<thead>
<tr>
<th>Investigation Request Date</th>
<th>Subject Imports</th>
<th>Investigation Findings</th>
<th>Presidential Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1978</td>
<td>Crude oil and related products</td>
<td>Imports threatened to impair national security</td>
<td>Imposition of fee on oil imports (later removed after court challenge)</td>
</tr>
<tr>
<td>1979</td>
<td>Crude oil and related products</td>
<td>Crude oil dependence upon Iran threatened national security</td>
<td>Termination of imports of oil imports from Iran</td>
</tr>
<tr>
<td>1981</td>
<td>Glass-lined chemical processing equipment</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1981</td>
<td>Ferroalloys and related materials</td>
<td>Imports did not threaten to impair national security</td>
<td>Upgrade of domestic stockpile and removed eligibility of ferroalloys for duty-free customs entry</td>
</tr>
<tr>
<td>1982</td>
<td>Crude oil from Libya</td>
<td>Imports threatened to impair national security</td>
<td>Embargo of imports of oil imports from Libya</td>
</tr>
<tr>
<td>1982</td>
<td>Iron or steel nuts, bolts and screws</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>Investigation Request Date</td>
<td>Subject Imports</td>
<td>Investigation Findings</td>
<td>Presidential Action</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1983</td>
<td>Metal-cutting and metal-forming machine tools</td>
<td>Formal investigation decision deferred</td>
<td>Conclusion of voluntary restraint agreements with exporting countries and launch of domestic industry revitalization plan</td>
</tr>
<tr>
<td>1987</td>
<td>Antifriction bearings</td>
<td>Imports threatened to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1987</td>
<td>Crude oil and refined petroleum products</td>
<td>Imports threatened to impair national security</td>
<td>No action to adjust imports, relying instead on energy security plan</td>
</tr>
<tr>
<td>1988</td>
<td>Plastic injection molding machinery</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1988</td>
<td>Uranium</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1991</td>
<td>Gears and gearing products</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1992</td>
<td>Integrated circuit ceramic packages</td>
<td>Imports were not a present threat to national security</td>
<td>Launched low-cost electronic packaging initiative</td>
</tr>
<tr>
<td>1994</td>
<td>Crude oil and refined petroleum products</td>
<td>Imports threatened to impair national security</td>
<td>None</td>
</tr>
<tr>
<td>1999</td>
<td>Crude oil and refined petroleum products</td>
<td>Imports threatened national security</td>
<td>None</td>
</tr>
<tr>
<td>2001</td>
<td>Iron ore and semi-finished steel</td>
<td>Imports did not threaten to impair national security</td>
<td>None</td>
</tr>
</tbody>
</table>

Although there have been legal challenges to several of the presidential actions noted above, only one wound its way to the U.S. Supreme Court. In *Federal Energy Administration v. Algonquin SNG, Inc.*, 426 U.S. 548 (1976), the Court was asked to determine whether the assessment of import license fees was consistent with presidential authority under Section 232 as delegated by Congress. The Court held that the President possesses the authority to adjust imports after a Section 232 determination by deploying non-quantitative methods (such as licensing fees) as well as quantitative methods (such as quotas), so long as the specific factors in Section 232(c) have been considered and so long as the President takes actions only to the extent deemed necessary to adjust imports to counteract a threat to national security. The Court further held that the authority held by the President was not overly broad in that the statute establishes preconditions for the exercise of such authority, including a finding by the Secretary of the Treasury that imports are threatening the national security of the United States.

The 1978 investigation of crude oil imports listed in the above table generated a legal challenge that culminated in *Gasoline Marketers Council, Inc. v. Duncan*, 492 F. Supp. 614 (D.D.C. 1980). In that case, the Secretary of the Treasury, acting pursuant to Section 232, reported to the President that crude oil was being imported into the U.S. in such quantities and under such circumstances as to threaten to impair the national security. Based upon this report, the President implemented a Petroleum Import Adjustment Program (PIAP) that added a conservation fee of 10¢ per gallon to the retail price of both domestically refined and imported crude oil. Because the PIAP fee applied to both domestic and imported crude oil, and because the fee would ultimately be paid by consumers of such crude oil, the impact would have been to lower domestic demand for crude oil regardless of its source. The PIAP was challenged as being a measure beyond the scope of the Section 232 powers delegated to the President by Congress. The District Court distinguished the PIAP fees in this case from the licensing fees in *Algonquin* by pointing out that the PIAP fee did not disadvantage imported crude oil (because it applied equally to domestic crude oil), whereas the *Algonquin* licensing fees applied only to imported crude oil. Rejecting arguments that the President had “inherent”
authority to act independently of Congress in matters involving national security, the District Court struck down the PIAP as a demand-side disincentive program too remotely related to impacts on imported crude oil and thus beyond the scope of powers delegated by Congress. As a result of this court case, President Jimmy Carter withdrew the PIAP conservation fee in June 1980.

The United States Court of International Trade (CIT) has already had an opportunity to give some consideration to the steel and aluminum tariffs implemented by the Trump Administration under Section 232. In Severstal Export GMBH v. United States, 39 ITRD 3084, slip op. 18-37 (Ct. Int’l Trade 2018), the CIT examined a motion for preliminary injunction filed by a U.S. importer of steel products and a related company in Switzerland (Plaintiffs) to enjoin the implementation of the Section 232 tariffs on steel imports, in part on the basis of claims that the President exceeded his legal authority to assess such tariffs. Specifically, the Plaintiffs asserted that the President misconstrued Section 232 by “over-reading what can constitute a threat to national security, in finding that steel imports currently represent such a threat.” The Plaintiffs further asserted that the present Section 232 steel tariffs are being “used in trade negotiations to draw concessions from other countries unrelated to steel imports.”

Citing Corus Group v. ITC, 352 F.3d 1351 (Fed. Cir. 2003), the U.S. Government took the position that the findings of fact and motivations of the Trump Administration in this investigation are non-justiciable matters. Nevertheless, CIT Judge Jane A. Restani proceeded to examine the investigation and exaction of tariffs on steel to determine if there had been a “clear misconstruction” of statutory limitations on the actions of the President.

Reviewing the Trade Expansion Act and in particular the factors that must be considered during the course of such investigations, Judge Restani noted that the BIS steel report referred to each such factor and that several of those factors are “economic in nature.” Judge Restani further stated that the language in 1862(d) is “quite broad and permissive, and apparently not limited to production necessary for national defense purposes.” Crucially, Judge Restani proceeded to state the following:

Plaintiffs have pointed to neither statutory authority nor legislative history which suggest that Section 1862(d) clearly forecloses the President from finding a threat to national security due to the overall economic situation of the steel industry. Where, as here, an industry is found to produce goods vital to U.S. national security … the court finds it highly unlikely that Presidential statements indicating an overarching economic rationale for Section 1862 tariffs are clearly inconsistent with that statute’s grant of authority.

Accordingly and unsurprisingly given this reasoning, Judge Restani held that the likelihood of the Plaintiffs succeeding on the merits of these constitutional claims was “very low.” Judge Restani ultimately denied the request for a preliminary injunction by the Plaintiffs.

Although somewhat truncated due to its procedural context, the analysis by Judge Restani in the Severstal case targeted some of the core constitutional questions pertaining to Section 232 tariffs. It also engaged Algonquin, the only U.S. Supreme Court case to directly address some of these foundational constitutional questions of presidential power. Future challengers of the steel and aluminum tariffs before the CIT will, at a minimum, need to fully consider the Severstal analysis and be prepared to methodically address its reasoning.

The U.S. Government will likely continue to take the position that these Section 232 tariffs are non-justiciable questions. Section 232 itself does not provide for judicial review, and presidential decisions under it are outside the scope of the Administrative Procedure Act. The American Institute for International Steel lodged a complaint at the CIT in June 2018, challenging this aspect of the current Section 232 tariffs as well as the constitutionality of the Congressional delegation of authority to the President that gave rise to Section 232.

V. THE CONGRESSIONAL RESPONSE

The implementation of the present steel and aluminum tariffs has generated a range of responses from senators and members of the House of Representatives, including the introduction of multiple and varied bills purporting to assert further oversight of the types of decisions that led to the imposition of these tariffs. For example, Senators Bob Corker and Pat Toomey introduced a Senate bill on June 6, 2018, which would require the passage of legislation by the Senate and House before the imposition of Section 232 tariffs based upon national security reasons. On July 11, 2018, a companion bill was introduced in the House by Representative Mike Gallagher and others that would similarly require legislative approval of such tariffs.

On August 1, 2018, a Senate bill was introduced that would relocate the leading Section 232 investigation role from the U.S. Department of Commerce to the U.S. Department of Defense (DOD), so that the DOD would have the leading
investigation authority to investigate whether imports threaten national security while the U.S. Department of Commerce would retain final remedy authority.\textsuperscript{45}

Clearly the subject of Section 232 tariffs has provoked sufficient interest on Capitol Hill such that, at minimum, the Congressional role over such matters is under renewed scrutiny. It remains to be seen how creatively and effectively Congress will continue to assert itself. The Section 232 concerns present an intriguing example of the delicate allocation of constitutional authority between two branches of government on a subject of global importance.

VI. WORLD TRADE ORGANIZATION CONSIDERATIONS

Beyond the legal considerations in the U.S., the Trump Administration’s steel and aluminum actions under Section 232 of the Act have predictably triggered reactions from many member states of the WTO. Although the WTO does not provide for private rights of action and thus is not open to private claims, the WTO Dispute Settlement Body is the ultimate government-to-government dispute resolution mechanism for disagreements between WTO member states over WTO-related trade law rights and duties. As such, it is indeed a crucial forum in which WTO member states can contest—and have contested—these Section 232 investigations.

The U.S. was a contracting party to the General Agreement on Tariffs and Trade (GATT) when GATT came into existence in 1947. In 1994, the GATT contracting parties agreed to a substantial revamping of the international legal framework for international trade, which resulted in the creation of the WTO. The WTO, which unlike GATT is an international organization, came into effect on January 1, 1995.

Like each GATT contracting party, each WTO member state agrees in principle to reduce its tariffs, non-tariff barriers and other mechanisms that frustrate the attainment of trade liberalization. A WTO member state can choose to do so for multiple reasons, including the relative opening of the markets of other member states to its exports and the benefits of mutual commitments to comply with other WTO rules-oriented agreements. To date, the GATT/WTO has proven to be quite effective at lowering bound tariff rates applicable to trade between its contracting parties/member states and these institutions have also achieved notable reductions in non-tariff barriers.

Recognizing that lowering tariffs and non-tariff barriers can in some instances require adjustments to domestic economic priorities and activities (adjustments that can be difficult if not painful for certain industries), the GATT/WTO approach has provided for limited exceptions to the overall philosophy of trade liberalization. One of these exceptions involves trade policies and practices that may be inconsistent with trade liberalization but which are pursued for national security reasons. It is this national security justification that forms the basis for the legal defense, thus far, by the Trump Administration of its Section 232 steel and aluminum tariffs at the WTO.

To fully contextualize the national security justifications at the WTO thus far by the Trump Administration, it is helpful to first understand the nature of the breaches alleged by other WTO member states. To date, the Section 232 tariff actions by the U.S. have generated nine requests for consultations, which is the first step in dispute resolution proceedings codified in the WTO Dispute Settlement Understanding.\textsuperscript{46} These requests for consultations have been lodged by China, India, the European Union, Canada, Mexico, Norway, the Russian Federation, Switzerland and Turkey.\textsuperscript{47} Many of these jurisdictions have assessed retaliatory tariffs against the U.S. in addition to seeking consultations within the WTO framework.\textsuperscript{48}

A common theme running through these requests for consultations is that the U.S. has taken measures in violation of its WTO commitments involving safeguard measures. A safeguard measure is an action (typically a quantitative restriction, \textit{i.e.}, a quota) that limits imports of items when there has been a large and unforeseen increase in such imports that causes or threatens to cause serious injury to the domestic industry of like or directly competitive products. WTO member states entered into an Agreement on Safeguards to benefit from a rules-based, and therefore more predictable, method by which they would launch a safeguard measure impacting its imports from other member states.\textsuperscript{49} Complaining member states have asserted that the Trump Administration is not actually taking action based on national security interests but rather is implementing safeguard measures.

Indeed, not one of the nine requests for consultations tendered thus far by WTO member states mentions national security considerations. As will be seen below, the silence on national security in these requests for consultations is nearly matched by the silence on safeguards in the replies thus far by the U.S.

In response to the allegations that it has violated the WTO Agreement on Safeguards (among other WTO commitments), the U.S. has thus far defended its actions as permissible under WTO Article 21. That Article, entitled “Security Exceptions,” originates in GATT 1947 and provides the following:
Nothing in this Agreement shall be construed
(a) to require any contracting party to furnish any
information the disclosure of which it considers
contrary to its essential security interests; or
(b) to prevent any contracting party from taking any
action which it considers necessary for the protection
of its essential security interests
(i) relating to fissionable materials or the materials
from which they are derived;
(ii) relating to the traffic in arms, ammunition
and implements of war and to such traffic in other
goods and materials as is carried on directly or
indirectly for the purpose of supplying a military
establishment;
(iii) taken in time of war or other emergency in
international relations; or,
(c) to prevent any contracting party from taking any
action in pursuance of its obligations under the United
Nations Charter for the maintenance of international
peace and security.50

There is no direct precedent of a GATT contracting party or
WTO member state using this Article to justify the imposition
of tariffs in the manner in which the U.S. has imposed its steel
and aluminum tariffs under Section 232.

By framing its actions in national security terms, the U.S.
essentially bypassed the principal article containing exceptions
to otherwise applicable WTO disciplines, namely Article 20.
That article provides grounds upon which a WTO member
state may base otherwise prohibited measures such as the
imposition of tariffs, non-tariff import restraints or export
restrictions beyond its WTO-committed levels.51 Article 20
does not mention national security but it does allow for such
measures where, inter alia, they are necessary to protect public
morals or when necessary to protect human, animal or plant
life or health.52 Interestingly, Article 20 also allows exceptional
measures when “necessary to secure compliance with laws or
regulations which are not inconsistent with the provisions of
this Agreement,” meaning GATT 1947 and now the WTO.53
It is telling that the U.S. does not attempt to justify its Section
232 tariffs on these grounds or on any other ground provided
for in Article 20.

The focus instead on Article 21 does, however, align with
several considerations likely of significance to the Trump
Administration. As noted above, the GATT/WTO dispute
settlement mechanisms have not previously been seized of the
issues related to the implementation of significant and across-
the-board tariffs of indeterminate duration justified entirely on
national security grounds. This lack of precedent was surely
known to the Trump Administration as it anticipated the
legal challenges that these Section 232 tariffs would trigger.
Moreover, the Trump Administration has been openly critical
of the WTO, and challenges to the Section 232 tariffs allow it to
invite (if not dare) the WTO to condemn as WTO-inconsistent
a U.S. statute colored as protecting national security.

The response by the U.S. to the request for consultations from
Switzerland is illustrative. That response, in part, states the
following:

The President determined that tariffs were necessary to
adjust the imports of steel and aluminum articles that
threaten to impair the national security of the United
States. Issues of national security are political matters
not susceptible to review or capable of resolution by
WTO dispute settlement. Every Member of the WTO
retains the authority to determine for itself those
matters that it considers necessary to the protection
of its essential security interests, as is reflected in the

Switzerland’s request purports to be pursuant to
Article 14 of the Agreement on Safeguards. However,
the tariffs imposed pursuant to Section 232 are not
safeguard measures but rather tariffs on imports of
steel and aluminum articles that threaten to impair
the national security of the United States. The United
States did not take action pursuant Section 201 of the
Trade Act of 1974, which is the law under which the
United States imposes safeguard measures. Therefore,
there is no basis to consult pursuant to the Agreement
on Safeguards with respect to tariffs imposed under
Section 232.54

Thus the U.S. takes the position that its Section 232 actions
are, in U.S. constitutional parlance, a non-justiciable political
question. Also on display is tension between a formal and
legalistic response by the U.S. (namely that the operative U.S.
statute is a national security statute and not a safeguard statute)
and a practical and commercial complaint by Switzerland
(namely that the measures taken by the U.S. are safeguard
measures notwithstanding the title given to them by the U.S.).55
The position thus far advanced by the U.S., however, is without direct precedent, and no GATT/WTO dispute resolution panel has concluded that Article 21 confers such unconditional discretion upon a contracting party/member state. The GATT/WTO jurisprudence on Article 21 is thin and the questions now pending before the WTO Dispute Settlement Body have never been fully addressed.

It is difficult to imagine that a WTO panel will agree that these Section 232 tariffs present jurisprudential questions over which the WTO has no jurisdiction. It is likewise difficult to envision a WTO panel not being troubled by the imposition of tariffs for ostensible national security reasons when those tariffs as applied have the practical impact of safeguard measures. Prevailing on these core claims could be a steep climb for the U.S.

In the event that a WTO panel does agree that these are measures governed by Article 21 (claims of national security) as opposed to the Agreement on Safeguards, it is doubtful that a WTO panel will concur with the U.S.’s assertion that Article 21 provides unfettered discretion to a WTO member state to unilaterally institute trade measures it deems in its national interest and that these measures are insulated from legal challenges by fellow WTO member states. The institutional ramifications of such a finding would be obviously detrimental to the WTO and to the overall project of rules-based trade liberalization. As an institution, the WTO is keenly aware of precedent and it is unlikely to legitimate a legal position that would usher in similar actions by other WTO member states and could ultimately pose a significant challenge to its core mandate. The fact that the U.S. has been a mainstay of the GATT/WTO system since 1947 and remains the largest economy in the world only exacerbates the dilemmas this matter presents to the WTO.56

In the event that the Section 232 tariffs are found to be inconsistent with the U.S.’s WTO obligations, the U.S. would be required to bring itself into conformity with those obligations (most obviously by withdrawing the tariffs in question). Should the U.S. not do so, WTO member states could begin the retaliatory process of withholding concessions from the U.S. until the U.S. complies with the WTO decision. While many WTO member states (including many of those seeking consultations over the Section 232 tariffs) have already implemented retaliatory tariffs against imports from the U.S., an official condemnation of the Section 232 tariffs would allow these member states to formally seek WTO approval for their retaliatory measures.57

There is substantial precedent for the suspension of concessions by WTO member states when the WTO Dispute Settlement Body has condemned the trade measures of other WTO member states but the offending member state refuses to bring those measures into conformity with its WTO commitments as determined by the WTO Dispute Settlement Body.

For example, in a dispute that endured from 1996 to 2012, Ecuador and other WTO member states (including the United States) challenged European Union practices related to the importation, sale and distribution of bananas within the European Union.58 In 2000, the WTO Dispute Settlement Body authorized Ecuador to suspend concessions to the European Union up to just over $200 million per year during the period of time in which the European Union did not bring its measures into conformity with WTO Dispute Settlement Body findings.59

Given the likelihood that the Trump Administration would not, in such circumstances, alter its investigation findings, legal determinations or ultimate trade actions under Section 232, it is highly probable that the U.S. is entering into a protracted period of public disagreement and legal dispute with fellow WTO member states over these issues. This suggests continued trade barriers with the accompanying increase in operational costs and decrease in market opening opportunities for affected companies and consumers in the U.S. and elsewhere.

VII. CONCLUSION

As mentioned at the outset, the Trump Administration has clearly taken dramatic steps involving international trade. The volume, rapidity and potential consequences of these steps have bordered on dizzying for attorneys working on matters related to them.60 At the same time, there have been few points in recent history in which persons involved in cross-border business have needed legal counsel on regulatory matters as much as the present.

It is clear that the U.S. is in a period of intense trade friction with many of its key trading partners. This friction will, as discussed above, place great tension on WTO institutions charged with settling disputes between WTO member states, including the challenges to the Section 232 steel and aluminum tariffs. The gravity of the institutional dilemmas facing the WTO due to the Section 232 steel and aluminum tariffs should not be underestimated. The disposition of these challenges by the WTO and the levels of compliance with such disposition by the U.S. and other WTO member states will likely play a large role in determining the duration of the tariffs as well as the duration of the measures instituted in retaliation to them.
Companies conducting business subject to current and future tariffs and retaliatory measures should expect heightened operational costs for as long as these measures remain in place.

Beyond friction in trade relationships and heightened costs for certain business activities, the current steel and aluminum tariffs shine a spotlight on the constitutional balance of powers between the Congress and the President. The system of checks and balances as related to international trade is being tested but not for the first time. It is likely that the single most influential factor that will ultimately determine the scope, duration and scale of the current and future usage of Section 232 by the Trump Administration is the strength and effectiveness of the reaction to it on Capitol Hill.

ENDNOTES


3 The Bureau of Industry and Security regulations outlining the conduct of such investigations are found at 15 C.F.R. § 705.1 et seq.


7 See Aluminum Report, supra note 5, at 2-4.


9 See id. para. 4.


12 U.S. Const. art. I. Other authorities frequently cited by Presidents to advance trade policies include the power to appoint and receive Ambassadors (Art. II, § 2 and Art. II, § 3, respectively) and the general executive power clause (Art. II, § 1).

13 See 19 U.S.C. § 1351. To illustrate the delicate balances found in such delegations, the Reciprocal Trade Agreements Act, despite delegating authority to the President to make trade agreements, simultaneously asserted Congressional prerogative by limiting the duration of such agreements to three years.


17 Id.


19 Id.

20 Id.

21 See Steel Report, supra note 5; Aluminum Report, supra note 5.

22 See https://fas.org/sgp/crs/misc/R45249.pdf.

23 Id.

24 426 U.S. 548, 559-71.

25 Id. at 559.

26 492 F. Supp. 614, 616.

27 Id.

28 Id. at 618.

29 Id. at 618-21.

30 It should be noted that the United States Court of International Trade is a fully empowered Article III district court with national and exclusive jurisdiction over key international trade legal questions, including the actions of United States Government agencies, with few exceptions. As determined by Congress, the jurisdiction of the CIT is set out at 28 U.S.C. § 1581. Such jurisdiction includes likely future challenges to

* Bob Bowen is Director of International Trade Compliance at United Technologies Corporation and leads activities to ensure compliance with the international trade laws applicable to its global operations. Bob previously served in similar positions at Avnet, Western Digital and Hitachi. In addition to private sector experience, Bob previously served in the U.S. Department of Commerce with a principal focus on World Trade Organization matters and U.S. international trade policy. He is a member of the State Bars of California and Michigan as well as the Customs and International Trade Bar Association. Bob has a B.A. from Miami University, a J.D. from the University of Detroit Mercy School of Law, and an LL.M. from Georgetown University Law Center.
the steel and aluminum tariffs assessed earlier this year under Section 232 of the Trade Expansion Act. Appeals of CIT decisions proceed to the United States Court of Appeals for the Federal Circuit.

31 See Severstal Export GMBH v. United States, 39 ITRD 3084, slip op. 18-37, at 2, 15.
32 Id. at 18.
33 Id. at 19.
34 Id. at 15.
35 Id. at 16.
36 Id. at 22. The Trade Expansion Act factors can be found at 19 U.S.C. § 1862(d). These factors include i) domestic production needed for projected national defense requirements; ii) the capacity of domestic industries to meet such requirements; iii) existing and anticipated availabilities of the human resources, products, raw materials and other supplies and services essential to the national defense; iv) the requirements of growth of such industries and such supplies and services including the investment, exploration and development necessary to assure such growth; and, v) the importation of goods in terms of their quantities, availabilities, character and use as those affect such industries and the capacity of the United States to meet national security requirements.
37 Id.
38 Id.
39 Id. at 23.
40 Id. at 25.
41 See 5 U.S.C. § 551 et seq.
43 S.B. 3013, 115th Cong. (2017-2018). That bill has been referred to the Senate Committee on Finance; the text of the bill is at https://www.congress.gov/bill/115th-congress/senate-bill/3013/text?q=%7B%22search%22%3A%5B%22title%22%5D%7D.
44 H.R. 6337, 115th Cong. (2017-2018). That bill currently resides with the House Committee on Ways and Means and the House Committee on Rules. For the text of the bill, see https://www.congress.gov/bill/115th-congress/house-bill/6337?text=true&%22search%22%3A%5B%22hr6337%22%5D%7D&rr=1.
47 See https://www.wto.org/english/tratop_e/dispu_e/dispu_subjects_index_e.htm.
50 https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI.
51 https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX.
52 Id.
53 Id.
55 As noted, the United States has requested WTO consultations with those WTO member states that have retaliated against the Section 232 tariffs. One claim by the United States is that these retaliatory measures, premised upon the alleged misapplication of the WTO Agreement on Safeguards, are without justification because the United States did not base such tariffs upon that Agreement in the first place.
56 Given that the WTO Dispute Settlement Body tends to move slowly and major disputes can take years to achieve final resolution, it is at least possible that the United States could withdraw some or all of its current Section 232 steel and aluminum tariffs prior to final resolution at the WTO.
57 It should be noted that the United States position that the WTO likewise lacks jurisdiction over tariffs would provide a basis upon which other WTO member states could argue that the WTO likewise lacks jurisdiction over their retaliations to such tariffs.
59 Id.
60 In addition to U.S. tariffs and retaliatory measures to them, practitioners must now also be aware of quota exclusion opportunities. In Presidential Proclamations signed on August 29, 2018, it was announced that the U.S. Department of Commerce will accept requests for steel products from Argentina, Brazil and South Korea to be excluded from the annual quotas for these imports established under Section 232 in June 2018. The same was announced for aluminum products from Argentina likewise subject to the annual quota mentioned above. See Presidential Steel Proclamation, supra note 8; Presidential Aluminum Proclamation, supra note 10.
IN THIS ISSUE

2 Welcome from the Journal’s Editor-in-Chief

4 Welcome from the International Law Section’s Co-Chairs

7 The International Law Section Continues Its Dynamic Relationship With Foreign Bar Associations Through Friendship Agreements and Conferences
   By Richard Bainter

8 2018 CLA Annual Meeting Report
   By Brian Arbetter

9 The International Law Section Presents Eighth Annual Warren M. Christopher International Lawyer of the Year Award

11 California Now Open for Business in International Arbitration
   By Howard B. Miller

14 SEC Confirms Its Authority In EB-5 and Tags Immigration Attorney for Unregistered Brokering in California Federal Court Win: SEC v. Feng
   By Charles S. Kaufman

19 Unarmed Attacks: Cyber Combatants and the Right to Defend
   By Anna C. Mourlam

31 Thief in the Night: The Invasive Nature of Home Internet of Things and Its Attempt to Silently Shift Rules of Personal Data Ownership
   By Celine Melanie A. Dee

43 Restorative Justice Solutions for Mass Incarceration
   By Jennifer Lim

53 Steel, Tariffs and National Security Under the Trump Administration
   By Robert Bowen