115th CONGRESS
*2nd* Session

Printed for the use of the
Commission on Security and Cooperation in Europe

# Roundtable on Illicit Trade

**JUNE 21, 2018**

**Briefing of the
Commission on Security and Cooperation in Europe**

**Washington: 2019**

**Commission on Security and Cooperation in Europe**
**234 Ford House Office Building**
**Washington, DC 20515**
**202–225–1901**
**csce@mail.house.gov**
**http://www.csce.gov**
**@HelsinkiComm**

**Legislative Branch Commissioners**

HOUSE
CHRISTOPHER H. SMITH, NEW JERSEY
*Co-Chairman*
ALCEE L. HASTINGS, FLORIDA
ROBERT B. ADERHOLT, ALABAMA
MICHAEL C. BURGESS, TEXAS
STEVE COHEN, TENNESSEE
RICHARD HUDSON, NORTH CAROLINA
RANDY HULTGREN, ILLINOIS
SHEILA JACKSON LEE, TEXAS
GWEN MOORE, WISCONSIN

SENATE
ROGER WICKER, MISSISSIPPI,
*Chairman*
BENJAMIN L. CARDIN. MARYLAND
JOHN BOOZMAN, ARKANSAS
CORY GARDNER, COLORADO
MARCO RUBIO, FLORIDA
JEANNE SHAHEEN, NEW HAMPSHIRE
THOM TILLIS, NORTH CAROLINA
TOM UDALL, NEW MEXICO
SHELDON WHITEHOUSE, RHODE ISLAND

**Executive Branch Commissioners**

DEPARTMENT OF STATE
DEPARTMENT OF DEFENSE
DEPARTMENT OF COMMERCE

## ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe (OSCE). The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

## ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

# Roundtable on Illicit Trade

**JUNE 21, 2018**

Page

## PARTICIPANTS



## OTHER PARTICIPANTS

Frank Cullen; Cynthia Braddon, Trace It; Kasey Kinnard, Financial and Outreach Coordinator, Terrorism, Transnational Crime and Corruption Center, George Mason University; John Kennedy; Gretchen Peters; Steven Sin, Director, Unconventional Weapons and Technology, Subject Matter Expert Instructor, National Center for Security & Preparedness; David Lynch, Director of Solutions, Sayari Analytics; John Pacheco; John Clark; Kristin Reif, Director Illicit Trade Prevention, Philip Morris International; John Clark; Susan Fridy, Acting Head of Center, Washington Center, Organization for Economic Cooperation and Development; Jim King; Rob Quartel, Chairman and CEO, NTELX; Tyler Crowe; Kevin Rosenbaum, Attorney, Mitchell Silberberg & Knupp LLP; David Luna, President and CEO, Luna Global Networks; Travis Johnson; Jon Kent; Blake Marshall; Chris Martin, Assistant Director, Fiscal Crime Liaison, Her Majesty's Revenue and Customs, United Kingdom; Jerry Cook, Vice President of Government and Trade Relations, Hanesbrands, Inc.; Liz Confalone; Kevin Delli-Colli, Managing Director, Forensic and Investigations Practice, Deloitte; James J. Duggan, Vice President, Coty Inc.; Flora Okereke; Clay Fuller, Jeane Kirkpatrick Fellow, American Enterprise Institute; Matthew Rubin; Crawford Allan, Senior Director, TRAFFIC, World Wildlife Fund; Dawson Hobbs; and Megan Glibin, Director, Customs and Trade Facilitation, U.S. Council for International Business.

# Roundtable on Illicit Trade

---

**June 21, 2018**

**Commission on Security and Cooperation in Europe**
**Washington, DC**

The briefing was held at 1:05 p.m. in Room 485, Russell Senate Office Building, Washington, DC, Paul Massaro, Policy Advisor, Commission on Security and Cooperation in Europe, presiding.

*Panelists present:* Paul Massaro, Policy Advisor, Commission on Security and Cooperation in Europe; Russ Travers, Acting Director, National Counterterrorism Center, Office of the Director of National Intelligence; Christa Brzozowski, Deputy Assistant Secretary, Trade and Transport, Department of Homeland Security; Lisa Dyer, Director, Office of Intellectual Property Enforcement, Department of State; and Aaron Seres, Acting Section Chief, Financial Crimes Section.

Mr. MASSARO. All right. So we've got a real full table today. I know everybody's shoulder to shoulder and everyone's going to get to know one another real well. You'll see, they pulled a fast one on us at the very last minute and gave us 12 mics, instead of the expected 36, so we're going to have to share. And I hope that's okay with everybody. But in any case, my name's Paul Massaro. I work for the Helsinki Commission and put together this event today. I'm going to go ahead and start with my opening statement, and we'll take it from there.

Good afternoon and welcome to this roundtable of the U.S. Helsinki Commission. The commission is mandated to monitor compliance with international rules and standards across Europe, which include military affairs, economic and environmental issues, and human rights and democracy. My name is Paul Massaro and I am the policy advisor for economic and environmental issues, including illicit trade. I would like to welcome you today on behalf of our bipartisan and bicameral leadership to discuss a topic fundamental to the national security of the United States and government based on the rule of law as a whole.

In the 21st century, criminals are hijacking globalization. By leveraging new technologies and exploiting archaic legal frameworks, transnational criminal networks have become a looming presence across the world. These networks engage in whatever nefarious activity makes them the most money. There is no specialization in the criminal world. Meanwhile, the rule of law, which has largely remained a national competency, struggles to keep up.

This is complicated further by the emergence of kleptocracies, authoritarian states that have merged with criminal interests and have at their core the personal enrichment of the autocrat and his cronies. It can often be difficult to tell where the public sector ends and the private sector begins in these kleptocracies. By taking advantage of this opaque structure and the one-sided openness of governments based on the rule of law where reliable information is readily available, kleptocracies profit at the expense of those who play by the rules.

The unique national security threat born of the merger of transnational criminal networks and authoritarian states is nowhere better expressed than in the booming enterprise of illicit trade, the topic of today's discussion. The damage done by illicit trade is immense. There is an economic cost, in the form of stolen intellectual property, lost sales, and tarnished brands. There is a social cost in the form of stalled development, environmental destruction and political corruption. Finally, there is a human cost in the form of those who are hurt or killed by counterfeit products, defective machinery, and deadly narcotics—not to mention those who have their lives destroyed through modern slavery.

The diverse group at today's roundtable represents a broad coalition seeking to combat illicit trade. We are joined by large companies, small- and medium-sized enterprises, universities, think tanks, trade associations, advocacy groups, and many other organizations that demonstrate the leadership and diversity of the U.S. private sector and civil society, and those of our allies. You all represent the prosperity and innovation that the rule of law makes possible. On behalf of our leadership, I would like to thank each of you for attending today. Each of your organizations is a valuable member in curbing illicit trade. And I encourage you to stay in touch with me and one another as we develop strategies to do so.

This roundtable is meant to signal clearly that the legislative branch, the executive branch, the private sector, and civil society are united when it comes to countering transnational criminal networks and their facilitators.

I have a short administrative note here about mic capacity, but I think I've kind of explained that already and we'll make do. So let me go ahead and introduce our panelists. Russ Travers will be our first speaker. Russ is the acting director of the National Counterterrorism Center. NCTC is responsible for leading and integration of the national counterterrorism effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure national CT objectives. Thanks so much for taking the time, Russ.

Christa Brzozowski will follow Russ. Christa serves as deputy assistant secretary for trade and transportation policy within the Department of Homeland Security's Office of Policy, where she is responsible for multiple economic and security policy issues that affect the United States. She is also the co-chair of the Organisation for Economic Cooperation and Development [OECD] taskforce on countering illicit trade. Christa, so glad you're here.

Ms. BRZOZOWSKI. My pleasure. Thank you.

Mr. MASSARO. We will then hear from Lisa Dyer. Lisa is the director of the Office of Intellectual Property Enforcement in the Bureau of Economic and Business Affairs at the Department of State, where she works with her colleagues to identify intellectual

property rights [IPR] issues and formulate strategies to engage foreign governments on issues of concern. Lisa, thank you. Trying to see you. Thanks for so much for joining us.

Finally, we will hear from Aaron Seres. Aaron is the acting section chief of the FBI's Financial Crimes section. Here, he oversees all of the FBI's financial crime programs nationally, which include a wide variety of fraud schemes as well as intellectual property crimes. He also has oversight responsibility for the FBI's Forensic Accountant Program. Aaron, it's a real pleasure to have FBI at the table.

Mr. SERES. Thank you. It's good to be here.

Mr. MASSARO. Russ, without further ado, the floor is yours.

Mr. TRAVERS. Thanks very much. It is a great pleasure to be here. Paul indicated I am a counterterrorism guy. And so that is going to be my optic as I talk about convergence. I'm going to do three things. First, I'm going to give you a little bit of nuance in terms of what convergence means from my perspective. Second, I will then burrow down into the relationship between terrorists and criminal actors. And then third, I want to give you a couple of very brief observations about how I think some of the lessons learned from counterterrorism over the last 17 years could be applied to transnational crime.

So, first, on nuance. A few years ago, we started talking about TCOs [transnational criminal organizations] and terrorism converging. That left the terrorism community a little bit uncomfortable. And definitionally, it would seem to suggest that they are coming together. And, kind of reduction ad absurdum, that al-Qaida was coming together with Russian organized crime, or something along those lines. And that clearly is not what's happening. Now, in our view there is a spectrum. On the one hand, you've got terrorists that definitely use crime, and have forever, for funding, logistics—Bali, Beslan, Madrid, 77—all, the entire spectrum. That motivation was ideological.

At the other end of the spectrum, you've got criminals who will use terrorist tactics for the purposes of intimidation. So that, for instance, you see Mexican drug cartels using beheadings. Their motivation is profit. And in the middle, you've got a whole host of kind of blurry interactions. You will have seen arrangements of convenience. For instance, Al-Shabaab and pirates a decade ago. You'll have fellow travelers. You'll have the Abu Sayyaf group in the Philippines, who are truly a bunch of thugs that wrap themselves in the Islamist flag. You might have AQIM, which is an amalgam of terrorists but also just long-standing smugglers. And then you've perhaps got the most complicated, which is Hezbollah.

Occasionally, you will get rather bizarre cases like that of Arbabsiar, who was convicted several years ago. He had a cousin who was Quds Force, Iranian. And he was trying to do the bidding of his cousin to reach out to Mexican drug trafficking organizations to eventually assassinate the Saudi Ambassador to the U.S. That's a little bit on the rarer side. The point is I think that you do have a very broad spectrum of interaction. And at least in our view, convergence as a bumper sticker kind of suggests a single narrative that we think actually is far more complex than that which may be concluded.

So what is going on? Again, from the terrorism perspective, there is no question that there is a nexus between criminal actors and terrorist actors in a number of different ways. I'll only give you two. First, we believe that terrorist groups knowingly exploit criminal activities for operational purposes, and they have done so forever. Interestingly, in the last several years you've also seen terrorists begin to provide a religious justification for engaging in criminal activity. Second, we find that non-ideological driven criminal

enterprises—such as human smugglers, weapons dealers, and document forgers—will work with terrorist groups solely for financial gain. Sometimes they're witting. Sometimes they're not. I want to address both of those in some detail.

So let's start with how terrorist groups knowingly exploit criminal activities for operational purposes. They tap into criminal networks or use criminal means to facilitate funding for the acquisition of materials or weapons. A few examples: To fund the majority of the group's operations, ISIS members have illicitly gathered and sold oil, pillaged antiquities, and they've extorted individuals in both Iraq and Syria. In a number of ISIS plots in Europe, the operatives tapped in criminal networks, including using personal relationships within those networks to identify co-conspirators and obtain fraudulent documents. It was pretty easy for them because if you look at someone like Abaaoud, who was responsible for the attacks in Paris, he had been a criminal. He had been in and out of prison. He had a very wide array of criminal contacts.

And it's not just ISIS. AQAP-associated attackers leveraged organized crime networks to acquire firearms to conduct the Charlie Hebdo attack back in 2015. And certainly, in Africa there have been concerns for years that extremists have supported financing group operations through illicit smuggling of everything from gemstones, to ivory, to charcoal. As Paul mentioned, the advent of technologically enabled services—dark web, digital currencies—have helped terrorist groups conduct their operations. They are quite good at exploiting the attributes of globalization and can move far quick than governments can.

An example: We had an al-Qaida supporter in Britain using stolen credit card numbers obtained on the dark web to generate more than $3 ½ million of revenue for the terrorist group. And a relatively recent EU commission study found that firearms acquired from criminal networks were a primary source of weapons for European terrorist attacks, all purchased on the dark web.

As I mentioned, interestingly, we started to see terrorist groups, through their propaganda, provide religious justification for engaging in criminal activities. ISIS has urged supporters to engage in criminal activities such as theft in Rumiyah and in multiple propaganda organs. In one article, ISIS argued that they should take wealth by any means. A prominent ISIS recruiter in Belgium said that stealing from the infidels is permitted by Allah and necessary to finance travel to jihadist hotspots. Amedy Coulibaly took out a consumer loan using fraudulent pay slips from a fake company to acquire over $30,000. He then used that money to purchase weapons.

The propaganda espoused tactics more commonly associated with crimes with a broad range of attack nodes. So within AQAP's Inspire magazine groups encouraged individuals to conduct arson, stabbings, and deliberate vehicle rammings, in addition to tactics more commonly associated with terrorism. And that kind of blurs the line for us in terms of determining motivation. Is it criminal, or is it terror? You'll also note that in publications like Rumiyah and Inspire, they use recruiting posters from organizations like al-Qaida and ISIS that advocate going after criminals to bolster their ranks—almost like an opportunity for redemption.

It's very common for individuals to start out in prisons as criminals, get radicalized, and go on to conduct terrorist attacks when they get out. And that is a trend that we've seen increasing around the globe. In the post-mortem for terrorist attacks, the individuals are often known to local security services as criminals, but not as terrorists. And that is a significant challenge for the intelligence community. An interesting guide point from the EU—last year a growing trend that ISIS had probably had the most success in exploiting

criminals to conduct attacks. Recruits are at least twice as likely to have a criminal record in the case of ISIS as they were in the case of al-Qaida.

So that's the terror side of the equation. We briefly discussed thoughts on how, when, why we believe criminal enterprises engage with terrorist groups. We believe the intersection between criminal enterprises and terrorist groups is largely transactional in nature and absent any common ideological views. Criminal enterprises will continue to place a higher value on the financial or material incentives they gain through various transactions over the actors that they are working with. In October 2017, a Pakistani national was sentenced to almost 3 years in prison for smuggling individuals to the U.S. At least one of them had family ties to the Taliban and who was implicated in a plot to attack the U.S. or Canada.

Several years earlier, three Pakistani citizens were sentenced to multiple years in prison for conspiring to provide material support to a foreign terrorist organization when they agreed to smuggle an individual who they believed to be a Taliban member. However, we've also seen many cases where criminals have been concerned that dealing with terrorists may bring unwanted law enforcement attention. So it's a bit of a risk calculus for them.

Criminal networks routinely conduct kidnapping operations targeting U.S. and other Western citizens. They also carry out kidnappings with the intent of selling the hostages to terrorist groups for financial gain, rather than any ideological motivation. A cooperative relationship between criminals and terrorists is, in fact, prominent in Afghanistan and Yemen, where foreign hostages often change hands between criminals and terrorist groups. The Taliban and Haqqani network in Afghanistan routinely cooperate with criminal groups and receive hostages from those criminal groups.

And that brings me to my last topic. I want to say just a quick word about the opportunities to apply lessons learned from counterterrorism to countertransnational organized crime. The nexus does have significant policy implications. Since 9/11, counterterrorism focus across the government has been very much focused on the whole of government efforts, better integration across the U.S. Government, to improvements in information sharing that may be horizontally within the Federal structures, vertically, Federal, non-Federal, with our international partners, and with the private sector. And it has involved the establishment of authoritative data bases and a completely integrated screening and vetting architecture.

It is not perfect, but we are dramatically better than we were 17 years ago. It has allowed us to push borders out. It has allowed us to keep potential terrorists out of the country, better track individuals, and build out networks. Many of these capabilities would be relevant to any transnational threat, but crime in particular, with better integration across law enforcement and intelligence across the United States, but also a better sharing of criminal history data with international partners. Judging from the improvements we've seen in CT, I think there will be substantial improvements in our understandings of transnational crime. And equally important, it would further enhance our own counterterrorism efforts, help plug a bit of a hole that exists as a result of this crime-terror nexus.

With that, I'll stop. And I look forward to questions after my colleagues.

Mr. MASSARO. Christa, please.

Thank you, Russ.

Ms. BRZOZOWSKI. Great. Thank you. So I will note start off with a little bit of a humorous note. The task for today is how to stop the flow of illicit goods. Not giving a sense of the problem, but just what is the answer to stop the flow of all illicit goods. And because it's not qualified in any way, I take that to mean globally as well.

Mr. MASSARO. I figure it's a pretty easy problem.

Ms. BRZOZOWSKI. [Laughs.] So I hope I have some good solutions here today. And I clearly don't have them, otherwise I would be on my yacht somewhere in the Bahamas. [Laughter.] I'm from the Department of Homeland Security [DHS], where I do trade and transport policy. And my usual disclaimer is have everyone emphasize the policy aspect of that. So please don't ask me any very specific questions about quarter rates or tariff numbers or the harmonized tariff schedule or anything like that. I'll know enough to get myself in trouble and not enough to actually answer the question. So we'll keep it at a pretty strategic level.

Within DHS, I'll give perhaps just a quick overview—although I'm assuming many of you, if not all, are very familiar with the mission of that department. It's always helpful to kind of give you at least my perspective so we're maybe starting off on the same page. The Department, as folks know, is a relatively new organization, a relatively still immature organization still figuring out how to integrate and how to work in concert with other Federal partners and other global partners. It brings together 22 different agencies that had previously been scattered across other departments.

And so it has a tremendously broad mission area that includes things as diverse as the counterterrorism mission that Russ was talking about, and it is focused on protecting critical infrastructure, including the broad transportation sectors, financial sectors, telecommunications sectors. So that mission set specifically for working with owners and operators and private sector folks is to protect those critical infrastructures here domestically. Also, a huge focus is protecting Federal networks and systems from cyberattacks—so putting out cyber guidance, hiring some of those professionals, and making sure that, first, Federal systems are secure, and then working and engaging with private sector folks to make sure that broader networks throughout the country are also secured and free from attack.

And finally, I'm giving you a high-level overview of the many, many missions in DHS—a big part of the mission is to facilitate the secure flows of goods and people. I'm here today to talk about the goods side of that house. That's my little niche of the world. But still, some pretty significant problem sets and challenges there.

So when we're talking about cross-border commerce, you'll usually hear about, customs—so Customs and Border Protection [CBP] or the Immigration and Customs Enforcement [ICE] folks. We get a lot of assistance from our science and technology people who provide and deliver some of the capabilities that are used. But ultimately, all groups come together within the Department of Homeland Security around the singular mission of supporting the vital economic benefit that we all derive from cross-border trade. We support it by both enforcing the number of laws that ensure both security and compliance and the revenue streams that continue to come, but strive to do so it in a way that doesn't impede free movement. That balancing act is one that we're constantly striving to maintain as we deal with goods coming across the border.

Here are a couple of stats just to put this in perspective. These are from 2017. So $2.4 trillion in imports and $1.5 trillion in exports are processed by DHS at the border

annually. That's across 328 different ports of entry, so a huge land expanse there as well. We deal with around 365,000 formal importers of records, folks that are actually accomplishing imports, and collect about $45 billion in duties, taxes, and other types of fees at the border.

If that wasn't enough, we—the DHS—are also doing that, hopefully, in close coordination with 47 different agencies that have some border responsibility or need for the data that is collected on the things and people that come across the border. This becomes immensely complex when, in addition to dealing with the flows of goods, you are coordinating with 47 different agencies, not only operationally but in terms of law and with their legal departments as well, as we are dealing with a huge amount of systems and capabilities. So there's a technology angle as well. We also deal with people actually working at the border. So a huge operational component there as well.

It's not an easy task on any day, particularly as we're in the midst of an evolving and dynamic environment the task is ever more complicated. DHS has a unique mission set and a unique set of authorities and capabilities working on behalf of all these different agencies. It is an area where the rules of the road and the lanes are being worked out on a minute-by-minute basis. But DHS is the biggest physical presence actually at the border. So we serve on behalf of these 47 different agencies to enforce compliance with laws that might not necessarily be DHS laws, but laws from the Department of Agriculture or the Department of Interior Fish and Wildlife Service.

We deal with everything from invasive species like a nematode to consumer health and safety on pharmaceutical or engine parts, to counterfeit and pirated goods, which we'll hear a bit more about today, to dealing with folks who are looking to misclassify or misvalue goods to avoid tariffs or duties or quotas or to claim preferential treatment, all the way to big, big concerns about the bomb in the box or WMD-type of weapons of mass destruction. Included in this is money, narcotics, weapons, and then a whole array of controlled technologies that are either conceived of or developed here in the United States, and that we just don't want to get in the hands of bad folks, and so we control those technologies for the purpose of export.

That was a quick overview of the diversity of the DHS mission set to again emphasize why I might not have all the answers on how to stop illicit flows. I thought I'd give you a quick overview of what that actually looks like and the challenge before us all. But I can give a sense of what the emerging and dynamic environment in the trade world looks like from our perspective. And as we've worked with many of you, and as we make sense of some of the evolving trends and look to characterize some of the flows and develop policies to address it, understanding the as-is and understanding the changes that are on the horizon is incredibly important. So I'll do that, and then outline some of the ongoing strategies and activities, not purporting to have all the answers, but some of the work that is being done and, in my opinion, should be done to counter illicit trade.

So on some of the evolving trends—I'm among an increasingly rare breed of folks that have been with the department since before it was the department—who came in with a new administration right before 9/11, and so had the opportunity to see this department develop, see the legislation that created it be worked on, see how the department has seen the issue of cross-border flows develop and mature, and see some of the priorities that we've had, some of the priorities I know Congress has had, and some of the priorities that I know industry has had change over the years.

I'll put two environments before you. First is the immediate post-9/11 trade which I'll juxtapose with some of the changes that we're seeing now. From there I'll address how those changes are impacting the types of illicit goods, and how that's impacting our strategies to counter those flows.

In the days right after 9/11, and probably even the years, the focus and the emphasis was very much on physical goods, stuff coming across the border, largely coming across in containers. You had a big maritime volume there, so lots of goods coming on big ships, either in bulk or in these big containers, from known retailers—the big importers, the big exporters, working through some of the big carriers. You had a focus then—I'm not saying other issues weren't important—but I recall many of the hearings, many of the meetings, many of the work with international partners tended to focus on this big bomb-in-the-box security concern. WMD, money, drugs, weapons, with a big import focus on security. The tools that DHS and other governments brought to bear at that time were based on the mantra of we have a risk-based, layered approach. We worked with foreign governments to push the borders out as far as possible and get as much information about entities and things as early in the process as we could to advance data. We used technology. And at that time, we were thinking about technology as scanners at the border to run goods through. And we always worked wanting to develop global standards.

In today's environment, I see many of those same types of concepts, but they need to be tweaked, evolved, or even, perhaps, developed wholesale, out of whole cloth, to accommodate the new world that we're in. Instead of just physical goods crossing the border, we see lots of services, lots of intangibles, transactions that are occasioned by not only globalization, but this move toward digitalization. We no longer see those giant containers, but rather e-packets, these small little things that I know end up on my front doorstep, more often than they should, coming from Amazon or other intermediaries. They're small, little packages.

We've got tens of thousands of new entrants to the marketplace, in addition to the big retailers, the big importers, the big exporters, you start to see more micro and medium and small business. And vendors or sellers that before had too many boundaries to participate in the global marketplace now find through digital capabilities an ability to do so. You therefore see a shift in some of the threats, at least from our perspective. And I'll put a big question mark over this whole area, because we're still making sense out of the threats in this space. But of course, intellectual property rights protection is a huge concern as we start to begin to believe that we're seeing, and are now working very hard to quantify, the growth of counterfeit goods and pirated goods.

That triggers consumer safety concerns, not knowing what is immaterial or where it's coming from if it is counterfeited, as well as economic concerns—not only to the brand owners, but to the taxes lost by U.S. Government, as well as concerns over where that money is going and what illicit activities is it perhaps feeding. There are a huge amount of data privacy concerns in this new world. This new marketplace runs on information. And as we've seen recently with Facebook, consumers and vendors have traditionally been willing to provide information on how to derive value from that information, how to tax that information, whether to tax that information, how to protect that information, and how to understand the future benefit of that information as we see the advent of big data analytics, as we see robotics, big data, and perhaps see the capabilities of our adversaries to suck in that data and potentially use it in ways that we can't even conceive of right now.

And then we also see the threats to the information and communication technology [ICT] that underpins this whole process itself, the component pieces that are being hooked into an increasingly globalized and interconnected information communication technology system that's the engine for this entire thing. What are its components? Who's producing them? What are their capabilities now and potentially in the future? These are things that are very much our concern here.

Many of the areas that we're working on are really to address this paucity of data, understanding the problem in this space. What are the new trends? What are the new risks? Who are the new actors? There is lots of work. You mentioned I was one of the chairs of the OECD Illicit Trade Task Force. Let me introduce my co-chair, Chris Martin, and former chair, David Luna. So we've got a font of expertise, mostly on that end of the room.

Mr. MASSARO. And the OECD is right there.

Ms. BRZOZOWSKI. And the OECD is here as well. Great. So sorry, didn't recognize you. [Laughter.] But organizations like this, like the World Customs Organization, are working to try to understand what these flows look like. We see assessments that are dated now, but that tell us that up to 2.5 percent of total world trade is in fake goods. We probably have newer numbers but I don't have them. And from that we see a lot of the innovative sectors being at high risk. And this is the bread and butter of the U.S. economy, is their innovation. When 6.5 percent of the trade in high-tech goods is fake, that's a problem not only for the producers of those goods and for innovation in general. Further, knowing and trying to figure out where are those fake pieces going is another major problem. Into satellites? Into nuclear plants? Into the defense industrial base?

We are also, through the OECD, starting to understand who are the players? Whose countries' rights are being infringed? What countries are doing it? Where are the hubs? And from there start to develop some very country-specific assessments. I point folks to the one that the OECD did of the U.K. that really tried to quantify some of the jobs lost, the impacts moneywise to the economy, as well as to specific companies of some of these flows. And it allows policymakers like myself to tease out areas where governance frameworks are most necessary. And we've been focusing on three areas: Understanding free trade zones and the impact that those zones and the policies and security features around those zones have on illicit trade. It's a little bit outside my wheelhouse, but our Department of Justice colleagues, and other legal folks around the world, look at the penalties and sanctions regimes that could be perceived as enabling this flow.And then finally I would like to focus on the term everyone's using these days, the tsunami of small packages or e-packages that are now hitting borders. We've got a significant amount of not only these small packages coming across the border, but just an alarming lack of global consensus around the basic things, like definitions, like advanced information requirements so folks can assess and target risk, around how companies should engage with governments. Where does liability lie for the movement of both goods and digital transactions? And then how do we collect revenue and who's responsible for it? So these are some of the big policy questions in the world on this issue.

So unfortunately, I'll leave you probably with a few more questions than with actual answers to them. But to the question of how to stop illicit goods, I think the old frameworks or the traditional frameworks still apply, they just need to be perhaps revised and some gaps need to be filled. It's all about whole-of-government approaches. It's about partnership with foreign governments. It's about understanding and using data, both to

understand the problem and then data to understand the movement and the actors involved. And it's about having the very best technology and resources from government and from the private sector to address the problem.

Mr. MASSARO. Thanks so much, Christa.

And we'll go to Lisa.

Ms. DYER. Thank you very much. And thank you to the Helsinki Commission and its staff for the invitation to appear today to represent the State Department's views on this very important topic. As you mentioned, I am absolutely honored to represent the State Department's Office of Intellectual Property Enforcement here today. Our motto: We represent America's genius to the world.

Why does the United States promote intellectual property protections in overseas markets? Quite simply: Intellectual property rights are an economic powerhouse. According to the Department of Commerce, 45 million U.S. jobs and $6.6 trillion of U.S. gross domestic products can be attributed to IP-intensive industries, as many of you in the room know. But small- and medium-sized enterprises, which represent almost 90 percent of all of the new businesses in the United States, also rely on IP protections to grow their business, to become stronger in our economy. These small- and medium-sized enterprises are also the highest percentage of new businesses in some of the emerging and developing countries around the world.

On a more serious side, supply chains that knowingly or unknowingly are including substandard counterfeit goods represent a real danger to all of us, as many of my colleagues have already mentioned. And that includes our soldiers, sailors, airmen and Marines. The dangers to the defense side is also equally as important. Pirated products transmit spyware, ransomware, and all manner of computer viruses, undermining the privacy and freedom of our electronic communications. At the Department of State, we have a special role to play on behalf of America's taxpayers. And I thank you for the opportunity to outline what we are doing to better combat violations of intellectual property protections and outline our suggestions to strengthen the U.S. Government's efforts in this area.

Our embassies are essential platforms for promoting innovation and intellectual property protections in overseas markets, as well as defending U.S. rights holders and combating counterfeit and pirated goods. The State Department's 1,500 economic officers posted worldwide ensure that the United States remains the world's strongest and most dynamic economy and help to ensure that global supply chains work efficiently, effectively, and responsibly. Each of these economic officers is evaluated on their efforts to promote intellectual property protections for Americans. What a tremendous resource for the American taxpayers—1,500 people working around the world to promote intellectual property protections.

Representing America's genius also means spreading the word. We show our foreign counterparts and public audiences that the United States economy is a strong example of the powerful gross domestic product building, economy expanding, job creating effects of strong intellectual property protections. We point out that if it works for us, it can work for them. But many audiences don't always see the connection between something as commonplace as a counterfeit purse or a pirated movie and the economic security of a nation.

The December 2017 National Security Strategy draws a direct line between economic security and this administration's national security priorities. For all intents and purposes, the document states that economic security is national security. It further states that we need to reduce the illicit appropriation of U.S. public and private sector technology and technical knowledge by foreign competitors. For those who are interested, it's on page 22 of the strategy. In my office, and more widely in the Department, we took this charge seriously. We've embarked on a new strategy that takes advantage of the strengths of all agencies and stakeholders to fight this battle. After all, there are no so safe counterfeit or pirated goods.

For those who don't know, our embassies are also staffed by representatives from a number of U.S. Government agencies who work with states' political, economic, and public affairs officers to promote intellectual property protections. Legal, law enforcement, and technical experts from the Department of Justice, the Department of Homeland Security, Health and Human Services, and the Patent and Trademark Office, among others, are key members of embassy working groups that are advancing intellectual property protections and fighting counterfeits and piracy.

I will agree adamantly with my colleagues that in the United States we all know that no one Federal agency can effect positive changes in tough policy challenges. By leveraging the strengths of a number of Federal agencies, but also you all in the room and those on Facebook Live, the U.S. companies and trade associations and small businesses, as well as our academic partners, we can make changes that benefit U.S. businesses and taxpayers. The U.S. Government doesn't have all the answers, and we'd be kidding ourselves if we thought we did.

Let me give you an example of how putting together the strengths of many agencies and stakeholders can effect positive change. Customs officials, as noted previously, are absolutely critical to stopping the flow of counterfeit goods into the United States and other countries. However, in many countries there are far too few customs officials that can adequately deal with this growing problem. We know this because our officers report these facts: What the word is about IP among citizens within their countries, where the government is putting their resources. And it's clear that many countries just do not have the right amount of customs officials to work closely with us.

To raise attention toward the role of customs officials, custom's top political leaders need to understand the importance of intellectual property protections. They need to understand enforcement as a way to counter the negative effects of counterfeit and pirated goods on the economy and, more importantly, on the health and safety of their citizens. Countries need to prioritize and allocate funds to increase the numbers of customs officials and to adequately train them. In some cases, legislative changes are needed.

Our ambassadors—political, economic, and public affairs officers—serving in embassies know enough of these top political leaders who have the power to make these changes. Our officers also know to include intellectual property in the broader economic goals of their host countries. And they are doing just that. Technical experts, legal and law enforcement experts, are also absolutely vital to this process. They can help write legislation, provide training to current and new customs officials, and work with the country's technical experts on a day-to-day basis to stop the flow of counterfeit and pirated goods.

You all in the room and other industry groups have developed on a voluntary basis a variety of best practices to combat counterfeits and privacy. And I wanted to highlight

just a couple of these valuable resources. The International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy has released several publications for a variety of audiences, ranging from landlords to property owners to governments and enforcements agencies. Its goal is to protect each member's grants and investments from the illegal practices of counterfeiting and piracy. If you haven't had a chance to look at their publications, I recommend you do so.

I'm also excited about the work of the Trustworthy Accountability Group and their Certified Against Piracy program. According to Mike Zaneis, the president and CEO of the Trustworthy Accountability Group, this voluntary initiative is designed to help advertisers and ad agencies avoid damage to their brands from ads placed on websites and other media properties that facilitate the distribution of pirated content and counterfeit goods.

We work closely with a number of other organizations. I'm a huge fan of the National Intellectual Property Rights Coordination Center, which just turned 10 years old this year. They bring together U.S. and foreign law enforcement officials whose common goal is to combat IP theft, actively reduce the flow of counterfeit and pirated goods, and to train domestic and international law enforcement officials. If you haven't had a chance to get to know these folks, I highly recommend you do. If we can do anything to help make those introductions, please let one of us know.

I will also acknowledge the OECD, the Organization for Economic Cooperation and Development. The works they've published on the flows of counterfeit and pirated goods are extremely valuable for, as Christa said, understanding just the staggering sums of money that are flowing across borders in the counterfeit space.

I've spoken about the talented people we work with to combat IP violations and reduce the prevalence of counterfeit and pirated goods. Now I will tell you how we protect intellectual property and thereby further the goals of the National Security Strategy. This year my team looked to our colleagues at embassies from around the world to ask them how we could help, but also understand the best practices that they embarked upon to just actually do what we've been talking about here.

Some of our indices have been active on these fronts in years, especially at some of the larger cities. They work closely with the top political leaders and their technical experts in those countries. But others have not. And we wanted to make sure that everybody had in their hand the right information and tools they could do to fight counterfeits and pirated goods. Based on the feedback we got from them, I'll touch on just three themes.

The first suggestion is disarmingly simple: Make it interesting and relevant to the audience. Illegal copies of music, videos, shoes, and even software can get into the hands of students all too easily. And that can begin a potentially lifelong habit of purchasing substandard counterfeit products. We tailor our public outreach activities to these very impressionable audiences. Most recently, our embassy in Cambodia hosted a panel trumpeting how IP enables musicians to make a living. They showcased the talents of a Cambodian pop star. The message was simple: If people don't pay for music, the musicians you love can't make a living. The event was streamed on Facebook Live and as of today has garnered over 41,000 views.

Another recommendation: That the Federal Government become fluent in emerging technologies, such as artificial intelligence, blockchain, quantum computing—any tech-

nologies that have the possibility to combat violations of IP protections and reduce the prevalence of counterfeit and pirated goods. Frankly, some of these technologies will not pan out or they won't live up to their hype. I have to say, though, if we do not have sufficient understanding of these technologies to have an informed discussion among ourselves with those of you in industry or with academia about them, how can we convince a foreign government that nurturing and adopting promising technologies that can help them in this space is beneficial for their economy and to help protect its citizens from harmful effects and counterfeit goods?

One foreign government official has already approached us asking: What do you think about artificial intelligence? What if this artificial intelligence creates some really important intellectual property? Who owns those properties? It's a great question. And an effort to answer these types of questions, or at least engage in conversations with them, continues providing our embassies with information to strike at the nexus of these leading-edge technologies and intellectual property rights. And we're doing so in plain language, because remember our audience. We are prepared to engage with foreign interlocutors on this front.

Most of the things that I talked about here are repeating what Russ and Christa talked about. It's about sharing information. We can outsmart the interconnected unofficial networks that facilitate and circulate illicit products by sharing information. We aren't perfect, as Russ noted. And can you imagine other countries, where the idea of talking to other ministries or other law enforcement or legal officials is an entirely strange concept to them. It's not easy, as we've seen in our own government, but we are continuing to work with our embassies to make sure that they understand the best practices that have worked elsewhere and trying to help them engage with those host governments, industry, and trade groups.

We share information for action to protect the health and safety of all citizens from the prevalence of counterfeit and pirated goods, and to improve the economies of countries around the world. On that note, this roundtable is an absolutely fantastic opportunity to establish this teamwork between government and business, and to build new understandings and partnerships. It's through these partnerships that I think we'll find the new tools that we can use to fight this difficult problem, to shut down illicit markets, put criminal entrepreneurs out of business, and help create a safer, more prosperous future for our citizens.

Thank you, again, for the opportunity to describe the outstanding work of our embassies, the Department of State, the private sector, and the technical experts from around the world in strengthening IP protections, thereby reducing the prevalence of counterfeit and pirated goods. I look forward to a productive discussion. And I, again, thank you.

Mr. MASSARO. Thank you so much, Lisa.

And we have our anchor here, Aaron, here from the FBI. Thanks so much.

Mr. SERES. Thank you, Paul. I appreciate it. And I realize it's between me and your questions, so I'll try to be brief. And I'll be probably echoing many of the sentiments of my colleagues that are here today.

Ladies and gentlemen, I thank you for the opportunity to speak with you here today about this important topic. My name is Aaron Seres, assistant section chief for financial crimes at the FBI. An expertise of mine is in financial crimes. So, for this past year I've been enlightened about the intellectual property crimes rights issues that are facing us

in this country. It'll be my pleasure here to discuss illicit trade, specifically intellectual property rights crimes. They have a profound effect on businesses and consumers alike.

The investigation of intellectual property crimes traces back to the beginning of the FBI in 1908, where our initial agents focused primarily on white-collar crime, one of those crimes being copyright violations. Copyright and patent clause of the Constitution has provided protection of intellectual property since the foundation of our country, recognizing the importance of such rights to encourage innovation and protect economic value for the United States. Our country showed great foresight in protecting these assets. However, I'm sure few could have imagined the growth of the intellectual property and the related crime problem facing us today in this interconnected global marketplace we all operate in.

It is currently estimated that intellectual property rights crimes generate approximately 461 billion dollars per year, a tremendous amount of illicit revenue for criminals, transnational and the like, to launder around the world in support of their criminal activities. Here in the FBI, we are a very broad agency. Just in the financial crimes section alone I have experts and specialists that assist us in money laundering and health care fraud to help us to support our intellectual property rights efforts. In addition to our specialists in intellectual property—many of them patent lawyers themselves in a prior life—we have experts in organized crime and our cyber division folks with technical expertise to help us with these upcoming technologies, such as virtual currency and the new platforms we see through the dark web.

You saw recently in the past year, the FBI and other partner agencies and international agencies have taken out some of these dark web marketplaces, which have been open forums for some illicit products and trade. But as our experts in the FBI and IPR have explained to me, that is not always the case with the products that we're talking about here today for you all. For you all, the products are so good and so well counterfeited they don't need the dark web often. They can trade over an open platform in the clear web, giving more credibility to the products that they're selling to consumers.

With the growth of the internet and ecommerce platforms, the opportunities for criminals to bring illicit goods to the market has grown exponentially. Criminals who once had to find ways to bring large quantities of fake goods into the United States now can direct ship to an unsuspecting consumer's home. This has lowered the barriers and costs for criminals who engage in intellectual property rights crimes, making these profitable schemes lucrative opportunities for transnational criminals.

Intellectual property rights crimes today are not only large in regards to the volume of illicit goods, but as our partners here have also mentioned, the potential harmful effects for our consumers, here in the United States and abroad. Counterfeits no longer just imitate popular clothing lines or the like. They now include items such as counterfeit pharmaceuticals, children's toys, and makeup with harmful toxins, fake airbags—all of which can lead to serious harm or even death to those consumers of such products.

The intellectual property rights program in the FBI prioritizes the investigation of theft of trade secrets, counterfeit products, and copyright and trademark infringement investigations, placing an emphasis on those matters that pose a threat to public safety and the health of our consumers and cases involving significant economic impact. However, we are not alone in this fight. These crimes are best addressed collaboratively with government agencies working together in a partnership with industry and foreign partners who bring all of our expertise and ideas to fight this crime problem.

I'm proud the FBI has such great partners as all of you here today, and many others who would partner with you. The FBI, along with our other founding partner, the Department of Homeland Security, and other partners in the National Intellectual Property Coordination Center, the IPR Center, which was mentioned by Lisa Dyer here just recently. The 23 agency IPR-focused fusion center that promotes national security through safeguarding of the public's health and safety, U.S. economy, and our military from predatory and unfair trading practices.

Through this center, which celebrated its 10th year back in April, government agencies are working together with our foreign partners, through Europol and others, to address IPR crimes. Although law enforcement efforts can have a significant educational and deterrent impact on the crime problem, we are greatly aided through the expertise, criminal referrals, and support of our industry partners. The FBI, with our IPR Center partners, participate in several national multiagency initiatives aimed at providing a comprehensive response to several high-priority counterfeiting problems.

One such initiative was Operation Ingenuity, formed to address counterfeit aerospace and automotive parts that pose a threat to human health and safety, such as airbags, brake pads, and the like. Through this initiative, law enforcement, working closely with a consortium of private companies from the automotive industry and e-commerce brought forth effective change, decreasing the supply of counterfeit airbags available to be purchased by consumers in online marketplaces. So the threat to the public has been significantly decreased as these potentially explosive devices are removed from our marketplaces.

Transnational criminals have expanded their counterfeit activities into all categories of merchandise with the primary purpose of generating criminal proceeds, with no regard for public health and safety. These criminal actors capitalized on the current ecommerce platforms available to sell counterfeit goods direct to U.S. consumers, capitalizing on copyright matters through illicit streaming services, and are targeting proprietary information to seek ransom payments for its return or to prevent release.

So how do we address these criminal organizations and individuals that manufacture and traffic counterfeit and pirated goods or other intellectual property? Similar to my colleagues here today, we will not have all the answers, but I think this is a great start. And I have some ideas from the FBI's perspective as to what we can do for good enforcement in IP. As law enforcement, we make good cases that will convict subjects, we have the handcuffs and we put the folks in jail. This is a significant deterrent for intellectual property rights criminals. Providing law enforcement deterrent to the crime problem is one solution, but we cannot arrest our way to a solution to the IPR crime problem. As mentioned and illustrated here today, it's going to take a village for us to address this issue.

One way we attack this problem is by addressing the supply and the demand for counterfeit goods. On the supply side, through interagency and public-private collaboration we have seen effective results in addressing counterfeits. The success in the automotive industry already mentioned, we have other similar initiatives to address counterfeit pharmaceuticals and to protect our U.S. Government supply chain. The goal on the supply side is to do what we can to create enough barriers to entry into the marketplace where criminals are deterred from trafficking in counterfeit goods. We will not stop all the flow of counterfeit goods into our marketplaces, but we can make it much harder for the criminals to make an entryway.

The FBI in this regard spends a good amount of time collaborating with the private sector through the IPR sector and various conferences, seminars, and events throughout the United States and the world. Here, the latest trends and best practices work to educate one another and find solutions to identify, disrupt, and dismantle counterfeit operations. Sharing best practices with companies can be one of our best tools to prevent proprietary information theft. As with all financial crimes, I always say the best victim is no victim at all. Right? I'd love to be there in all situations. And the more we can get toward that goal the better.

Our companies are on the front lines facing criminals—you all are seeing this from a front row perspective—seeking to steal their information. And there are efforts that have been taken in regards to compartmentalizing your production, your manufacturing, your sales, ensuring your human resources are putting in strong noncompete nondisclosures, exit interviews are being completed of individuals, and there's a robust structure to monitor and track activity of folks within your private entity. Much as the case with the FBI, the biggest threat often to the loss of information in our IP is an inside threat from folks who work in our companies or have worked in our organizations. We must be diligent in protecting from this threat.

It's also critical for law enforcement and the private sector to build relationships, so that in the even if there is an incident or response there can be a response as quickly as possible. Similar to a kidnapping event, we see the theft of intellectual property from a company in a similar situation in terms of the need for speed to try to get back the intellectual property that was taken from you. The faster that law enforcement is made aware of an issue, the more effective we can be in assisting a private sector company.

On the demand side, public awareness campaigns are very important to educate consumers on the risk of fake products. I will be the first to admit that I did not have breadth of the mass amounts of counterfeit products that are out there prior to my current role here in Washington, DC. And it is immense. We live in a digital society where consumers—including myself, including people in our families and families around the world—our consumers are used to searching the web for the best price for the item they want to buy. They just want to find the best opportunity at the lowest cost, and then it's shipped direct to their door.

However, there may be a reason that price is so good, and it's not for the benefit of the customer. The more we can educate consumers, the better. For some products the message is safety, as we discussed in regards to the airbags on our auto parts, toxic toys, and the like. But in other areas, like fraudulent, illicit streaming, we must educate the public on the risks of the illegal streaming boxes and their services. These devices can be a gateway for criminals not only to make money off of individuals, but potentially allow them access to your network and your personal information that can lead to further victimization.

I believe it's messaging through ways like this where we can reach these consumers with a message that is important for them. We would not just leave our front doors open for all to enter, and that may be exactly what's happening with some of these products. In addition to addressing supply and demand, criminals cannot get their fake goods to market without private sector intermediaries, such as online marketplaces, payment processors, different companies. The FBI has worked with these industries on education and these entities have their own form of monitoring, looking for indicators of IPR crime, and are making referrals to law enforcement.

Criminals are often, though, the early adopters of new and a disruptive technology and will seek to exploit vulnerabilities when they can. The sharing of information amongst y'all in industry, amongst law enforcement, and amongst foreign and U.S. partners is vital for us to connect the dots—not just identify a bad vendor, but the network behind it is critical as we work together to disrupt and disband these operations, protect IP, and keep consumers safe. We go around the world not only training and providing outreach with private sector folks and individuals, but also with our foreign partners.

Just recently, we've had a request to go to Europe—over to Eastern Europe, to the Middle East, and other locations around the world to provide training on organized crime, corruption, and intellectual property rights enforcement. Sometimes those are basic, building the foundation for these other agencies, other law enforcement to assist us in these efforts. Sometimes it's more advanced. But I think these efforts are going to work over time, and we're trying to see some fruits of our action. In addition, the FBI has deployed around the world 63 legal attaché offices and works very closely with our partners in Homeland Security, Department of State and others, on continuous education and law enforcement efforts around the world.

One issue that I would like to finally note here is the pervasiveness of the intersection between transnational organized crime and the counterfeiting. What we're seeing is not just the trafficking of the counterfeit goods into the United States for the purposes of profiting these organizations. It's also a tool and a vehicle for agencies and entities, such as the Mexican mafia and Los Zetas and others, drug trafficking organizations south of the border, that are not only trafficking counterfeit goods or profits—such as DVDs and other Motion Picture Association issues—but also to use those as a vehicle for trade-based money laundering to move funds across the border through the United States and other countries.

The FBI is committed to addressing this issue, not only going after the counterfeiting but also trying to address specifically these professional money laundering facilitators that are out there to provide the facilitation of illicit proceeds, regardless of source, around the world for a fee. And we are seeking to hold the individual companies that are out to steal your IP rights accountable for their action. As given in a recent example up in Milwaukee of a wind turbine investigation related to the company by the name of Sinovel, who acquired wind turbine technology from a U.S. company, resulting in hundreds of jobs lost, hundreds of millions of dollars in lost funds to that U.S. entity. There was a very successful investigation. It resulted in a conviction of a foreign company, who sought to shortcut their efforts by stealing the properties of a U.S. company, and sought to advance their efforts and cut out the U.S. partner.

These are just a couple examples of what we're seeing across the globe. I believe that what we're all echoing here today is that partnership amongst the folks in this room, amongst the folks in the world are the most important efforts we can make in addressing this problem. I appreciate the time to discuss this important topic and I look forward to our discussions here today.

Thank you.

Mr. MASSARO. Thanks so much, Aaron. Do you mind if I take a microphone now?

Mr. SERES. Yes, sir. Here you go.

Mr. MASSARO. [Laughter.] Thank you. All right, so for the discussion section, here's how we're going to proceed. If you could place your nameplate like this if you'd like to

speak. We're going to go left to right around, Okay? If you have a question or if you have a comment, if you can just please keep it to about 5 minutes. We'll just keep going around left to right, in that order, until we've exhausted everybody's time and patience and/or we've hit 4:00 p.m., all right? Okay, great. And please also if you're asking a question, if you could let us know who you're asking it to—one, two, three of the panelists, whatever—that'd be very helpful.

Okay, so we're going to start right there. Clay, if you could just state your name and organization.

Mr. FULLER. Thank you. Clay Fuller with the American Enterprise Institute. I'm a Jeane Kirkpatrick Fellow in foreign and defense policy studies. I specialize in authoritarian political institutions.

I'd just like to start off quickly by saying to all our panelists, and to Paul, and to everybody at the table, thank you for everything that you do that makes America the greatest, most prosperous, and most powerful country on the planet in the history of Earth. I mean, I think that's awesome. And I think we need to make sure we don't lose sight of how great everybody is at what we are actually doing. That's not to say that there's not problems. There are lots of them. But America is also the best at always solving them, so we'll get to work.

Forgive me if I put on my professor's cap for a second. It'll only be a second before I have some questions and policy stuff. But in thinking of this in the connection with kleptocracies in particular, I don't know that there's such thing as an authoritarian regime out there that's not a kleptocracy. They are all kleptocracies in my view. But, again, you could debate forever over what's what. Is democracy in decline? All this stuff.

So I'll go with illicit trade, illicit finance are both forms of corruption, right? But if you ask, what is corruption, right, every single person that you ask is going to give you a very different answer. Corruption is typically perceived through the eye of the beholder, through the eye of the victim typically. This is why we have such a diverse crowd from very diverse sectors all around the table, which we could have representatives of every agency of government that deal with aspects of this, because it's a very, very—in social sciences, we call it fuzzy. A fuzzy concept.

So if we all agree, though, we want to fight illicit trade, we want to fight illicit finance, we want to combat corruption, it's useful, I think, to think about what the opposite of corruption would be? Which is something I don't think we do very much, and it's important to do. I hope whatever the opposite of it is, is what we are fighting for. We have to have something that we're fighting for, right, if we're going to successfully get rid or something or weed it out.

Most people fall back on the rule of law definition, right? But this is an equally fuzzy concept, right? Whose laws? What rules? Where? The questions could go on forever. So to make it simple, start with Transparency International. Their most basic definition of corruption is the abuse of entrusted power for private gain, right? Reverse that, and you get a definition: the use of earned power for public gain, right? So the use of earned power for public gain. If you think about it, earned power—it could be considered to be somewhat synonymous with private enterprise, right, especially as it relates to trade and finance, right? But it could also be reputational power, such as in the media or in nongovernmental organizations, right?

And then if you think of a term for the use of earned power for public gain, public gain can be considered synonymous with the benefits of living in a democracy, which we all enjoy—the prosperity, the freedom, the stability and the strength of living in democratic countries. With this, we can start, I think, thinking clearly about policy objectives and ways to structure our conversations around this. I'd call it a guiding principle. So if you want—if you take that reverse definition of corruption and you want to fight illicit trade, then that means it can be fought by increasing more opportunities for rules-based trade. We fight illicit trade with more rules-based trade.

Specifically, this means expanding our own foreign trade zone program, modernizing, growing it even more, publicizing it more, bringing more of the private sector into them to increase our exports, to increase our imports, and to grow our trade program will minimize the size of the illicit sector. It will actually provide opportunities for illicit actors to join the actual licit market. Internationally, through the State Department we could move to improve compliance standardization around the world through the OECD recommendations that are out there right now. There are special economic zones all around the world that grew Dubai from a bunch of mud huts into the beautiful spectacle that it is today, right? Grew Tianjin into the beautiful skyline that it is today, right? But they need some rule of law. There needs to be some help there to get in compliance standardization around the world so that we can all respect our own—the privacy rights.

Specifically thinking of illicit finance, there are things we could do at home such as beneficial ownership registries I think are a very pragmatic start that Congress could do that would give the executive agencies a tool not only to enforce the law but will also lighten the load on compliance departments of our banks, and would actually lighten the load on the compliance departments of small banks, which would actually allow small financial institutions to actually compete better in the game. So you combat illicit finance by creating opportunities for more licit finance.

In my expertise, it might be helpful to reevaluate the way sanctions work as well too, because there's actually a conundrum when you enforce sanctions—which I'm not against sanctions, I like sanctions—but when you enforce them, it actually creates illicit trade. It creates—North Korea has to go around them. And this creates networks. This creates illicit trade highways that criminals and terrorist organizations can jump on and use as well. And so we can recognize that in sanctions legislation and actually design ways to get into countries that are being sanctioned and help them facilitate better rules-based trade.

So I'm curious if you have thoughts on where that fits into your specific agencies.

Mr. MASSARO. Any particular person, or the whole panel?

Mr. FULLER. The whole panel.

Mr. MASSARO. Thanks, Clay. Let's just go left to right here, Lisa to Aaron.

Ms. DYER. There's a lot there. [Laughter.]

Mr. MASSARO. Clay always gives us a lot to unpack. [Laughter.]

Mr. FULLER. Sorry.

Ms. DYER. I think I'm going to defer my response to Christa, because I think some of her—[laughter]—I think some of her remarks actually touched on a few of the items that we talked about with free trade zones, and her remarks about sanctions. So I will defer my time to her.

Mr. TRAVERS. And I'm afraid it's not really a terrorism or intelligence question. So I'll pass it along.

Mr. MASSARO. [Laughter.] Christa's very on the spot.

Ms. BRZOZOWSKI. Man, thank you. No, very interesting comments. I was particularly taken with your thought that you have to figure out the opposite of what it is that you're coming to oppose, therefore bringing something to the table. Actually wrote that down. It's going to inform some problems that we're having with international organizations as well, and that you can't just say no as we're trying to tell you something. We actually have to have something to hold up as the best practice or as the standard.

On illicit finance, that area is not really my area of expertise. But I think some of your comments about the kleptocracy and the figuring out what these finances are actually funding and how they are funding it is—it's an interesting framework. I don't think we've written a lot on this. Some of those recommendations might be helpful to digest a bit more in a written form.

FULLER: There's a report coming out soon I'll be happy to share with everyone. [Laughter.]

Ms. BRZOZOWSKI. Yes, perfect. I'd invite you to also take a look at a report either coming out or just recently came out from the OECD, where they are looking at what happens in those foreign trade zones/free trade zones. And a lot of the illicit finance, a lot of the figuring out who's who and what corruption is and how it's defined are issues that were discussed. This report doesn't necessarily purport to have all the answers, but it does provide guidelines. And so, but if it's not final yet, it's in the state of being released for public comment and input. I'd invite you to take a look at that as well and maybe some of the intersections and the ideas—[inaudible].

Mr. MASSARO. Aaron, you do finance, right?

Mr. SERES. I do. Yes. [Laughter.] That's right up my alley.

Ms. BRZOZOWSKI. Should have started at this end. [Laughter.]

Mr. MASSARO. That's true enough.

Mr. SERES. Right to left. On the issues of legislative affairs, I would defer to our partners at the Department of Justice. But I would make a comment from a law enforcement perspective, we are seeing a lot of increasing professional facilitation of money laundering and individuals who are, in the business of moving money around the world for a fee. It used to just be a guy who was connected maybe an organized crime family or some other group with criminality. And now it's very professionalized. In that regard, any tools that we would have at our discretion to allow us to do our job better in that space are always welcome. One challenge for us nominally is trying to trace through the funds, through a multitude of shell entities and other structures where the money moves from place to place. So just in regards to your beneficial ownership comment, any tool in that regard for law enforcement to utilize is a helpful tool.

Mr. MASSARO. Thank you very much, Aaron. Let's move to the next speaker, right over there. Jerry.

Mr. COOK. Thank you. Jerry Cook with Hanesbrands.

Let me start with thank you for what you all do and your teams do, because we need a very strong U.S. Government. And we need you all to employ the best people with the greatest acumen in what you do. And we need you to share that, use that, and help defend us along the way. And we share a lot of risk. And we share risks sometimes not

with y'all, but with others. And one of the things in our company, we were one of the original CTBAC, Counterterrorism and Business Against Smuggling. But we do not share any risk data or any risk situations with a single foreign country. We will only share that directly with the U.S. Government and no other.

And we have a policy not to allow the U.S. Government to share anything we share with them to a foreign government. And our experience has been no good deed goes unpunished by a foreign government. And that includes the kidnapping of our management team—not just senior but low level—and other things that happened to them in this process. So the first thing we run into is, our people are most important to us. It just seems too often we find ourselves in a situation where once we leave the U.S. shore the criminal element, terrorist element, whatever you want to call it, we have no government.

I've dealt with nine kidnappings, and there is nobody that comes to your rescue. You're on your own. It doesn't matter if you're in Haiti, Colombia, if you're in Jordan, if you're in Brazil, or if you're in Mexico. There is no government that's there with you on that. And that's a big issue, because you talk about real threat and intimidation. It is a real threat and intimidation when one of your peers has been taken.

The second item I'd like to point out is there is no universal definition of illicit trade. So if you picture going hunting, and someone says, look, we're going hunting and we're going to go out. What are you hunting with and what are you hunting? Are you hunting deer or rabbit? Are you hunting criminals? Are you hunting terrorists? So that's a very big issue for trying to narrow down what you're chasing.

But the one thing that we've learned overall is that in the world that we live today it seems that the one caution that we would flag is that the U.S. Government has—like businesses—sometime we're overdriving our headlights. And we're doing that right now in the world of ecommerce. The ecommerce sphere, you compare—I'm moving a container, let's say 10,000 pair of underwear coming into the United States. Hopefully you're all wearing it, and if you are you're comfortable. [Laughter.] If you're not, we can fix that. [Laughter.]

But one of the challenges you have is that you know everything about who my manufacturer is, where my manufacturer is located, you can see us. You can look on Google Earth and watch. You can see a lot of those things. You can see my containers move, see where I'm shipping to. But in the ecommerce world, you don't know any of that. You know there's 50,000 people in a container. It was said earlier, and it's true, a container catches the U.S. Government through enforcement when it's one person bringing it in. But if there's 50,000 different entities in it, the government doesn't care about the 50,000. It's too small to go after one person, but who do you go after?

So those tend to become an accelerator. Why that's important? If they're in a free zone next door to us, doing bad behavior, you're bringing bad behavior into a free zone that I'm trying to defend, keep clean, and keep the other people out of. And so we operate in certain free zones around the world. We're large enough to keep other people out, not for competitive reasons, but for security reasons. We will only use a certain class of carriers off the seaboard and only certain airlines. And we won't use others.

The third item is time. The way the government's working today with data, you're making us hurry up and wait. The TSA is a good example of that. So if I'm shipping something by air, or if I'm shipping by ocean, I've got to hurry a container to a point to have it sit there for 2 days. It is open for anybody and their brother to grab that container.

In the days that we used to, we could take a container, be the last one on board, drive it to my plant. We used two different security groups plus the government. It would go straight on. No one could touch that. So we have increased the danger for the shipper, we've increased risk for the U.S. Government, and we've increased risk for our own nation by having this pause process. If I give you data, you can see it moving by GPS, just pick—[inaudible]. We'd like to slide that data model over to y'all. Y'all picked it up and it's coming straight through because you can move and move faster.

The other one is that when it gets down to it, when there's a failure there's only one person that loses in a failure—the company. We get fined. Somebody stows in a container, someone smuggles drugs in, the government fines us. No U.S. employee loses their job. No government employee gets fined. Only a company gets fined. Then we can advertise in the newspaper: Somebody found marijuana. So when you pull all that down, there's a hybrid inside the government today that's called Customs and Border Patrol. They've been through so many wars with companies like us. They have an incredible intuitive knowledge base. They've taught their people how to work tightly with industry. We share data. They share.

But we have backed away from government sharing risk to us now. So we don't get a risk profile. You're sharing it with other governments, but you're not sharing it with us. And the compounded problem now is you're also sharing all of my shipment data. You publish it. [Inaudible]—gets it. It's enough that Jon Kent's here. It's enough we share all that with our broker. You make our brokers go through a lot of background checks for employees because they have intense data. And they have a lot of exposure if they have bad employees. And so we have good brokers.

And when you share our cargo information, which you do, you release it and organizations like yours publish it, you will allow every drug cartel, every smuggler to mimic our cases, our quantities, from what location. And then the last piece that goes with it, we used to never tell anybody where we were shipping through. We'd ship from a foreign location. We'd tell the carrier to go to a certain port. But we would never tell you where it's being distributed to. Customs would know through a third-party paper to them.

The trucker would never know which trucker is picking you up, because we use the roulette wheel, so that they could never—the cartel could never go to the trucking firm and go after them, because we knew if we kept that silent—the only reason they're going to try to use our supply chain is if they know they can get the drugs out. So the more we could control, not knowing where it's going to and who's going to get it, that now is a requirement. We have to tell you where it's going, who's getting it, who the driver is. And you've put all these people at risk in the process, maybe for good reason.

But our request to you is, let's go back to the world of intimacy. We will give you everything you want, but don't make us tell everybody else and don't share it with everybody else. We trust you. We want you to trust us. But we don't trust the process today that's so public. And the other is, we really need the random factor to be in there. But we also need to respect the people that make the product around the world that are put in harm's way, whether it's criminal or terrorist, because they no longer pay people off to do something wrong. They hurt them. And they disappear. And that's our concern. We got 74,000 people around the world. We don't like it when they disappear. We don't like it when somebody doesn't come to work. We are very aware when you don't show up for work today, it's probably not because you're sick. It's probably because somebody has

threatened you and you have chosen not to be disloyal to the company, so you just don't come to work. So we need your help. And we need to do this together. The process today I think is a little misdirected.

Mr. MASSARO. Would anyone on the panel like to respond? Maybe Christa, or—yes, Russ?

Mr. TRAVERS. I'll start. So after 9/11 I was one of the deputies at the NCTC. And I was given the charter of trying to figure out how we had improved information sharing. I didn't know anything about the subject at the time. I've now been in the government for the better part of 40 years. So I'm pretty convinced that information sharing is more complicated than any intelligence discipline I've ever been involved in. Your points are fascinating, and I would frankly love to follow up. The NCTC doesn't deal a ton with the private sector. I think we have gone miles in terms of fixing department-to-department information sharing. But we're not as good at the Federal to non-Federal. And while we try to push out more information to the private sector, that tends to be a little bit more DHS and FBI than statutorily my remit.

But I could certainly bring together the relevant executive branch organizations to sit down and talk about pairing with the private sector, what you give us, what we give you. The international thing is a huge challenge. There's no question that when it comes to terrorism our country can't do it alone. And so we are absolutely having to deal with lots and lots of other counterterrorism-focused countries around the globe. We try to do it smartly. So we share a lot more with our very close allies and we share a lot less with those that we may have interests that overlap. But I take your point. I don't know the private sector in particular, but it really plays into that. So I will get your card and exchange notes.

Ms. BRZOZOWSKI. Yes. I mean, yes, very compelling points, Jerry. Being responsible for 74,000 people across a global footprint sounds like an extraordinary challenge. And when you're dealing with people's lives, it's going into a whole new terrain.

I guess from the DHS or customs perspective in how we see the world, I'll take on your point regarding this very sensitive shipping data and some of the vulnerabilities that it produces for your folks and also for your product. Perhaps it's helpful to look at some of the issues in the regulatory data. So what's required per regulation, which has gone through a formalized public comment review process where we take into consideration a lot of the points that you're making, and the voluntary data, which is also positive and can be the germ of later, smarter, more informed regulations. I think the CTBAC might have even started out as a voluntary partnership before being regulated. And you see other types of programs that DHS has for getting advanced information, programs which start off as a voluntary exchange of data to figure out what makes sense, who has what when, who can share it through what means.

And so grouping those two things—regulatory and voluntary—when you're talking the regulatory data, in terms of the shipping data, there—it is an interesting conversation that I'd love to continue as well. You've got—on one hand, you do hear industry wanting some sharing of that customs data between administrations through formalized processes and mutual information-sharing agreements so that there's some consistency as you're trying to get stuff across borders, and that some of the countries that could benefit from the information that we're seeing—there's benefits to business of that sharing as well.

So unpacking that—where there's benefits and then when does it really start to become dangerous, I think, is a very interesting question. We see really tangible benefits in sharing among allies, be it the Border Five or Five Eyes or all these different acronyms, to compare notes—where new threats are coming, where new actors are, and expanding each of our regulatory reaches. Kind of dividing that—finding that line of when it slips over to too much, I think, is a big, big concern.

And then I'll just touch quickly on the provision of this voluntary data, because I do think that's something that we're wrestling with right now as a matter of fact. Customs and Customs and Border Protection, as you said, and DHS, have a really solid, decades-long relationship with industry and there is a trust that I hope we've developed over those years. That's not to say that we should always be requiring or asking for voluntary data. Voluntary could very easily slip into de facto required. I think we appreciate that. So we ourselves need to be disciplined. And then we also need to be disciplined when we're establishing global standards and talking about provision of voluntary data, And the default of exchanging everything and opening the kimono to everyone may be something that's attractive to some when you're talking about the United States having that relationship with businesses, when we're talking about adversaries having that relationship with U.S. businesses, requests data from U.S. companies to get access to other markets, it's not a voluntary request anymore. So maybe just some thoughts there.

But I think from the shipping-data angle, I'd push back just a hair and say there is a real and demonstrated value to governments sharing that information, but we've got to make sure we've got that calibrated correctly so it's not leaking out to places where it shouldn't.

Mr. MASSARO. Great. Thanks so much.

Let's have the next speaker here. Chris, please.

Mr. MARTIN. Thank you, Chair. I'm going to make an observation and then ask what I think is a rhetorical question.

Mr. MASSARO. Please, real quick, get your full name and organization. [Laughs.]

Mr. MARTIN. All right. Yes, I do beg your pardon. Sorry. I'm Chris Martin. I represent the U.K. customs and tax administration here in Washington, but I'm also speaking on behalf of the OECD Countering Illicit Trade Task Force.

So I'll make an observation, I'll ask what I hope is a rhetorical question. I think to the point made by Mr. Cook about how there is no definition of illicit trade, I think I'd just like to say that it's been an asset to the OECD Countering Illicit Trade Task Force that we didn't tie ourselves down too firmly to a definition. By keeping it broad—by keeping the task force focused on all aspects of illicit trade from counter-narcotics, people smuggling, alcohol, tobacco, pharmaceuticals, wildlife products—keeping it broad meant that we attract the broadest range of stakeholders to the task force—law enforcement, NGOs, industry, academia. I think that's to our advantage.

The question of free-trade zones, I'll say there's no smoke without fire. Back in 2008, the Financial Action Task Force on Money Laundering recognized the vulnerabilities in free-trade zones, and prior to that the World Customs Organization. And there have been some excellent reports since that time: World Customs Organization; Europol; Interpol; the Business Action to Stop Counterfeiting and Piracy [BASCAP]; and very recently, of course, the TRACIT report, the Global Illicit Trade Environment Index, which includes five free-trade zone case studies, which are excellent. Of course, free-trade zones, offer a

preferential environment for businesses to thrive, to attract investment and innovation. But those same benign circumstances and environments—lack of taxes, duties, bureaucracy, and oversight—have allowed illicit actors to thrive in those zones.

And as a consequence of that, and building on all of the work that others have done in the past, the task force has had a sharp focus on the lack of transparency in free-trade zones and what we might do about that. Working with the European IPO, we've developed a code of conduct, voluntary guidance for governments and free-trade zone operators. That guidance will be released to public consultation in the very near future.

So my question to the panel, and to everybody else here actually, is: When that public consultation is launched, I would ask you to please take part of that. The more evidence and the more responses we can get to that, the greater weight we have in implementing something which is absolutely necessary to improve transparency and governance in free-trade zones across the world.

Mr. MASSARO. Thank you.

Yes, you want to have everybody respond to that, Chris?

Mr. MARTIN. Maybe [just a little ?].

Mr. MASSARO. Okay, just to nod your head yes, everyone. Okay, got it. [Laughter.] Perfect.

Okay. David?

Mr. LUNA. Thank you very much, Paul. My name is David Luna. I'm the president and CEO of Luna Global Networks, a former U.S. Government employee for the last 20 years working for the executive branch, started my career here in the U.S. Senate.

Let me first start by applauding Senator Wicker and his co-chair, Congressman Smith, for their leadership in encouraging his staff in organizing this very important illicit trade roundtable. The U.S. Helsinki Commission is a very unique mechanism that, as you said, Paul, is bicameral as well. And it's great to see the executive branch here, and I applaud the administration and my former colleagues for being here on this important roundtable.

I do also recognize and applaud the support of the private sector and civil society organizations for being here. It's not only the whole of government, but really it's the whole of society that I think is important to tackle the illicit trade.

As we have learned from the important research of the OECD, we're finding more and more about the breadth and scale of today's illicit market. It's really in the trillions of dollars, as we heard at the opening, and it's getting worse. Whether it's in counterfeits—I know from the IDSA [ph] and the ICC BASCAP project that the value of the counterfeiting and pirated goods will double in 5 years. And I think if we look at the issue of cybercrime, it will go from $1.5 trillion to $3 trillion in 5 years as well.

So I think it is a very important time to be discussing these issues with the administration. And, I think the question that I had is in February 2017, President Trump issued a very important executive order to combat transnational organized crime. And we've heard a little bit from NCTC on the overarching National Security Strategy. We also heard from DHS.

The specific question that I had: Is there any effort within the administration to do a deeper dive in developing an anti-illicit-trade strategy to help not only work with the private sector, but with other partners overseas to combat these threats? We heard on

how free-trade zones are becoming more and more important as a conduit to various illicit criminal activities.

And related to that, I think the resource issue is becoming important. I know that the OECD has also undertaken an exercise of case studies for intellectual property. And I think it would be great if the United States were to follow on those case studies and join other partners, helping partners like Panama in their capacities in the Colon Free Trade Zone so that they can fight corruption and the various illicit activities that are going on in Panama.

And finally, I think public-private partnerships are very important, and I would hope if there were to be any strategy that we could leverage and harness the expertise and resources of the public—or the private sector as well. Thank you.

Mr. MASSARO. Fantastic.

David, anyone in particular you want to hear from first there?

Mr. LUNA. Well, I mean, there's four and they represent the administration. So, as a followup to the executive order, whether there's any effort to do a specific strategy to combat the illicit trade——

Mr. MASSARO. We'll start from the left. Lisa, you got anything to say on that?

Ms. DYER. I will defer to Russ. I mean, his——

Mr. MASSARO. Great.

Ms. DYER. His organization has a very strong lead in that area—[inaudible]—activity.

Mr. TRAVERS. I would just say, David, as I think, when the last strategy was done on transnational organized crime, it explicitly noted that our efforts against that problem suffered after 9/11, that we—from my optic for the intelligence community, we cut back on both analysis and production related to transnational crime to move resources to terrorism.

I do think it's fair to say that, as you've seen in the National Defense Strategy, that terrorism is no longer viewed as the Number 1 priority for the country. I completely agree with that assessment.

When it comes to transnational crime, within the intelligence community it's absolutely fair to say that there is now greater focus on the problem, and that within the interagency there—the executive order has spawned a number of very senior-level meetings to figure out how exactly do we handle prioritization and mission management and those sorts of things. I can't say—and, frankly, I just don't know—whether or not there's a new strategy on the horizon. But I take your point entirely that the executive order, I think, has reflected a new focus—a renewed focus on the problem at hand, and that's just a really big deal.

Mr. MASSARO. Next speaker, please.

Mr. LUNA. Just one followup, related to that. On the resource issue, is there an effort to work with Congress to try to earmark or get more resources to combat illicit trade and organized crime?

Mr. TRAVERS. In that regard, you're now way out of my lane. That would be Department of Justice and Department of Homeland Security.

Ms. BRZOZOWSKI. Yes, I will say that—just, again, back to the definitional issue. On illicit trade, I don't think anything is specifically earmarked. But you do see requests—and I don't want to get ahead of any new budget items—but reflective of the most recent

president's budget that came out, new moneys are requested from DHS specifically to help implement the Trade Enforcement and Trade Facilitation Act that came out in 1915, but was started to be implemented in 1916. That covers a lot of issues that I think would be germane to this umbrella title of illicit trade, forced labor, human trafficking, import safety, IP violations, and other types of trade issues that are perhaps less specific. So in that regard, yes, there was a wholesome DHS-wide request of resources to make sure that we've got that customs presence that we noted was so important.

And then I'll also note, too, that we're very interested—we haven't cracked this nut yet—in finding ways to better understand the IP-specific impact, as I noted in my opening comments, to the U.S. economy, and find ways to potentially have the OECD assist us with the work and have a resulting document similar to the one that I think the U.K. has and that's been valued by them and which has benefited them enormously in being able to tailor very specific policy and operational responses because they've had that quantitative data and are able to use that as the basis for action. So in that very specific regard, yes, but watch that space.

Mr. LUNA. Great. Thanks.

Mr. MASSARO. Thanks so much.

Please.

Mr. ROSENBAUM. Thank you very much. My name is Kevin Rosenbaum. I'm an attorney with Mitchell Silberberg & Knupp LLP, and I represent a coalition of the copyright industries. I am here in my individual capacity, though, so these comments may not reflect my clients. Just to get that set. [Laughter.]

Mr. MASSARO. Okay.

Mr. ROSENBAUM. So, again, thank you for having me. I've enjoyed the discussion so far. In particular it was great to hear a lot of talk about the dangers of digital piracy, which is what I spend a lot of my time worried about, and in particular how digital piracy websites are sources of malware and funding for criminal networks, and of course damaging very much to the economy.

And I think, for one, I just wanted to make a fairly brief comment. I think in the early days of the internet there was this notion that the rules don't apply to some things online—that piracy, we should just kind of look the other way. I think that has slowly changed. I think there is a growing recognition that principles in the physical world should be brought to bear in the virtual world.

And we've heard a lot of talk about it taking a village and this being a group effort, and one group I wanted to make sure we note here is the role of internet platforms and intermediaries. Just like how in the physical world landlords can't look the other way while counterfeiting is happening on their sites, the same principles of liability needs to be looked at for internet platforms that may look the other way or not take appropriate action to prevent illicit activity on their sites.

And in foreign countries where piracy rates are sky high, a lot of times these countries do not have adequate principles of protection or liability, and that is a huge problem that I see around the world. And then I think it's a problem that our trade policy really does not adequately address. So I just wanted to kind of note the role that these internet intermediaries have in this discussion, and to mention that principles of intermediary liability that are at least as strong as what we have here in the U.S. should be very important to promote overseas as well.

Mr. MASSARO. Thank you, Kevin.

Christa, would you like to comment on that?

Ms. BRZOZOWSKI. Yes, thank you so much. This issue of intermediary liability is one that's very timely right now. We're looking at this as an interagency and finding ourselves at tension with some of these principles, meaning these very questions that you had noted on, which physical-world principles and rules apply to this new world? Where is a tweaking necessary or where is a wholesale new way of looking at it in a transformational way necessary? And that's exactly what's happening literally today in organizations like the World Customs Organization, that we have a working group on e-commerce that is looking at these very issues.

I'll just give you a little sense of the conflict as we see it—not necessarily an answer, but maybe some input from you during or after on whether we're conceiving of this in the right way. I hear your point that liability should be with the platforms, the marketplaces, and that is a thought or a way to do this. But really they're pushing back a bit. And their defense is you've got to understand that business model, and there's very specific ways that currently laws are enforced, compliance is enforced, revenue is collected, and then often it's associated with who is formally designated in certain capacities as the importer of record, for instance.

As these value chains and supply chains become even more attenuated and you've got a whole bunch of new actors, you've got some new models that countries are looking at—Australia, the EU, China with the Alibaba model—that are very, very different. And some of the questions we have to ask ourselves is that pro/con analysis. Making the intermediaries liable and asking them to do more about the safety of the products and the intent of the players using their platform is one thing, and there is value there. It assumes, though, or is predicated, I think, on those intermediaries having access to more information. And if, again, you flip that prism, we're now potentially asking U.S. companies and U.S. citizens to provide a whole bunch of data to platforms that probably have closer relationships with governments than our U.S. platforms do.

And so what are the security implications there? What are the business implications? What are the consumer privacy, what are the market access implications? Is this veiled tech transfer? So those are the two sides that are at tension right now, even among us in the U.S. Government as we try to work to establish global standards.

So I take one—I take the point I think David—or Jerry had made earlier of you can't just say no, you've got to come with an alternative. And so that's very, very much front and center—I mean, that's what we're working on among the interagency, key players being Treasury, from the revenue angle, DHS, State Department of course, Commerce, and then FTC, of course, because of the consumer safety and anti-competition law angle of what is the U.S. policy and position on this, and should we be piloting concepts of how best to leverage this immense power of these new players of the intermediary platforms.

Mr. MASSARO. Yes, please, please.

Ms. DYER. Thanks for your remarks. For those of you who aren't aware, I will tell you that the United States Trade Representative's Notorious Markets List that comes out annually contains information from our embassies overseas. One of my colleagues reaches out to them to say what online and physical marketplaces are you all seeing as you are living in those countries that we should be worried about, that we should identify as places trading in counterfeit goods or listing pirated content, for instance. And we make

that information available to the entire network of government agencies, taking a look at that information, and together with work from your organization helps to create that Notorious Markets List, and for those who haven't seen it, it's available on the United States Trade Representative's website.

Our embassies are really focusing on trying to shut down some of these digital piracy websites. I'm delighted to say that our embassy in Vietnam just had a major success in shutting down one of the largest pirated websites. The government of Vietnam made that happen thanks to the intervention and the conversations that our embassy had with the government.

We are actively working with other governments around the world to do the same thing, and you will forgive me if I don't tell any more details because these sites are slippery little suckers. [Laughter.] We close them down in one place and they pop up on a server in a different country. It's extraordinarily difficult, but that doesn't mean that we don't pay attention to it. So I wanted to just make sure that we let that we are actively working on it.

Mr. MASSARO. Thanks, Lisa. Rob, please.

Mr. QUARTEL. I'm Rob Quartel. I chair NTELX, which is a technology company that does autonomous decision management systems for the government, including FDA, and [predict O&I ?]—you and Customs are an indirect client, British Customs—the former Federal maritime commissioner, and sit on a number of technology boards including the Center for Innovative Technology out in Northern Virginia which has two funds, one of which is a cyber fund.

And I have a couple observations and a question, and one is that I've been hearing the issue of data since about 2001 when I first brought the idea of container security as an issue to Customs and some of the working task forces, and of course the issue then was that the industry, with which I was very familiar, didn't trust Customs to secure their data, and yet they were being told they had to give their data to Customs, including some that was voluntary, and Customs has now, for 17 years, been unable to bridge that gap between industry and the data collectors. And it's a huge problem partly because there's a dilemma involved in it, which is that we use a lot of that data for high-level commercial decisionmaking and the analytics, and companies like Haines use it for tactical security. So that one has not been solved in all of this time.

The bigger issue, I think, is the technology one. Lisa, you mentioned that you all are looking at things like blockchain and all the rest of that. I see these technologies every day—blockchain and many others, quantum computing, et cetera. I deal with that. And it seems to me—and this is my suggestion—if you are not doing it, you and the DHS should—and I know the NCTC is doing some of this, but government agencies never can keep up with what's happening in the private sector on technology. There is always a lag—always a lag.

So I don't know if you have, but you should have an industry-based technology committee that people who actually are on the front lines of technology development—not to have a Cisco or whatever company—because they are not doing it. You ought to have a working group that deals with technology advancement in both of your situations, and you may already have it.

So that's a suggestion, and I don't know if you have.

Mr. MASSARO. Does anyone want to comment on that?

Mr. QUARTEL. Let me make one more point about blockchain.

Mr. MASSARO. Sure.

Mr. QUARTEL. We all tend to think of blockchain—all we who are in business—as a solution to security, but it's also a solution for the guys—the bad guys, particularly if it's combined with pneumatic [ph] data—not nemetic [ph], but pneumatic [ph], which is miming real data at the outset of a blockchain pathway.

So it's both a good and a bad.

Ms. DYER. I will be honest. I'm not aware of an industry-based tech committee that's advising the U.S. Government on it, but it's a great suggestion. I've said it's fascinating to see the claims of what blockchain is going to solve out there, the environmental challenges associated with blockchain and the amount of energy required to make that work on a global scale I think is something that I'm really looking forward to learning more about—whether it actually is a viable solution for some of these, so thank you very much for your suggestion, and that should be a great one.

You may know something else, Christa, that I don't know.

Ms. BRZOZOWSKI. I don't know anything specific to blockchain or some of the technologies you mentioned. I know enough to be dangerous, again—[laughter]—but without having the answer or relationships with the Office of Science and Technology Policy at the White House, or OSTP—I mean, they do a lot of the engagement across the administration on making sure that we're connecting with industry.

I've benefited from some of their engagements so I know their work, so we probably do need to query them and see specific to this set of problems that we're looking at, what are some of the solutions.

I have to admit I've received—it's got to be dozens of briefings I'm watching right now, and I still don't get—[laughter]—how it works, and I do have a natural skepticism that I would need to overcome on how is this just not the next silver bullet that 2, 3, 4, 5 years from now we're going to understand how it could be used—not only by the bad guys but attacked and delegitimized by folks having access to it in ways that we just haven't thought of today.

So, yes, helpful solution, and I think we've got a couple of calls in to OSTP to point us in the right direction.

Mr. QUARTEL. If I can add, it's not just blockchain. That's just the symbolic technology. I think there are numerous technologies——

Ms. BRZOZOWSKI. Yes, the autonomous decisionmaking—yes, absolutely.

Mr. MASSARO. Okay, thank you so much. We'll go on to the next speaker. Susan?

Ms. FRIDY. First of all, I'd like to say I'm really grateful to have heard a couple of the speakers already mention the OECD. I should say I'm Susan Fridy, the head of the OECD's Washington Center, so hopefully that's already putting in people's minds that the OECD is a key partner for working on these issues.

Our secretary general likes to say that global issues require global solutions, and I think this issue is one that certainly exemplifies that. And I also like the phrasing that David Luna used a few minutes ago, saying that we need not just a whole-of-government approach, but a whole-of-society approach.

So I just want to make a plug for the OECD's role in this because I have a colleague here from the U.S. Council for International Business, which is the formal U.S. business

arm of the OECD. So, if you are a business representative, you should talk to the U.S. Council for International Business—USCIB—about how is it that business can work with the OECD and work with other international organizations as well on this and other key issues. And there are also ways that civil society and labor can participate with USCIB, but I think on this issue especially, the private sector really ought to be having a good, strong voice, and showing governments—not just the U.S., but other governments that are members of USCIB, what are the key issues that you are facing every day, the kind of conversation that we're having here today is crucial for letting policymakers know what is happening on the ground, what are you seeing that they might not be aware of.

So I think my question for the panel is along those same lines, do you see how the private sector could be more engaging, I think maybe especially for Lisa and for Christa, since you are familiar at least with the OECD through the task force and through other work? I know business is involved, but how do you think that they could be more involved with international fora?

Mr. MASSARO. Thank you, Susan.

Ms. DYER. I know that we very firmly support having U.S. business at international organizations. It is a fundamental tenet. We are delighted when people do join us at those organizations.

I am incredibly grateful for the number of people who come to us and say, hi, can we talk, can we share what we know and what we've seen so that it better informs your work. I know that it takes a lot of time to get to the Department of State, to get through the security, but thank you for doing that.

I also want to say, please, when you are traveling overseas—if you don't already—please stop in to see the embassies. Again, it's not easy, but the more they know about your challenges, the more people in Washington hear about them because they let us know that you've stopped by and you've made your issues known. It makes them smarter and more capable to—hey, I have an upcoming meeting; I might be able to raise this with my counterparts over there.

And then I will just say that I am grateful for the questions and the comments here today. I have learned a tremendous amount from each one of you, and I look forward to the rest of the questions.

Mr. MASSARO. Thank you, Lisa. Christa?

Ms. BRZOZOWSKI. Yes, very quickly, and thank you again for all the excellent help from the OECD. We rely on a lot of that data that comes out of the organization very extensively in my work.

So how best to plug in industry? I mean, again, you can make millions off that if you came up with a perfect answer. [Laughter.] I've got a couple of thoughts because from the very beginning my work in trade and supply chains is vitally dependent on input from industry and across the spectrum. And I find two things extraordinarily valuable. One is when you are having a formalized conversation with industry—and by formal I mean on a specific issue, or with a specific agency—some internal consensus or a prioritization done by industry of self-organizing before or as they engage with government is really helpful.

What can be difficult for government stakeholders who are not experts in each of the areas that everyone else is is to have—roundtable discussions like this are great when we have a diversity of thought and opinion, but prescriptive do this, do that, government

can fix the problem, coming from various voices without being prioritized can increase the noise-to-signal ratio. So formal advisory committees are also extraordinarily valuable. There's a process then by which there is some self-vetting among the industry, some consensus emerges, and what issues are the most important and how they should be prioritized, and how they should be teed up for government stakeholders to consider.

So in that regard I would say, those formal pathways are very, very important, but we also very much appreciate these types of less formal and also just we pick up the phone and call us so that we know—we have a network of folks to call up—hey, I've got a question, who might know that answer.

I'll give an example. USCIB and Harry [sp] have put together, and the Chamber, a session for interagency stakeholders, government folks before we sent a team to the current meetings in the World Customs Organization that I just mentioned so that we could talk about the agenda and get that perspective from our various industry stakeholders. So that kind of very agile/flexible hey, tell us what you think on a particular issue, that was a bit outside of the formal advisory constructs that government has but are a bit more of a listening session for government to just be informed and updated by the industry perspective. So just a couple of ideas.

Mr. MASSARO. And let me also say just from the Helsinki Commission perspective, we want to hear from you, too. [Laughter.] The legislative branch has to play our role, so you all have my information; now please reach out to me, my interlocutors on the committees, and things like that. We've got a role to play in this somewhere.

So, all right—oh, Aaron, yes, please.

Mr. SERES. I just want to echo what Christa was saying—we do a lot of outreach with private sector entities. A lot of them have interests when they have overseas assets or deployments of operations forward in another country—what do you do, how do I go about that, how do I assess the risk—so any international outreach to that extent is helpful to these companies. And when I do outreach like that I implore them, as Lisa and I go to the embassy, make a contact, find individuals who are on the ground, where you are putting your assets internationally. And then here locally those forums are great for companies who share information about best practices or what they're seeing.

And what Christa mentioned about the coalition of industry—in the automotive industry we talked about the success against airbag products that are defective and others. And there is an entity, A2C2—it's a coalition of automotive industry that brings together one voice for that industry to help message to us and message to other entities, what their issue is as an industry. So I would second that that is a great way to go about it if they've been dealing with a government entity and trying to get a message to law enforcement, trying to get some effective change from a working perspective.

Ms. DYER. May I——

Mr. MASSARO. Yes, please. Please, definitely.

Ms. DYER. Jerry, your comments about the safety and security of your people, I'm sure that is shared by everyone here. If you haven't had a chance to join the Overseas Security Advisory Committee that Diplomatic Security in the Department of State runs, I urge you to do so.

When you are traveling overseas you can easily register that you are traveling, or your employees can register when they're traveling. It helps them when an emergency takes place—whether that's a political coup, or some humanitarian or natural disaster

that hits. Immediately our first priority is supporting American citizens overseas when something like happens. But our job is more challenging if we don't know that you are there. So please, if you have a chance to do that, I urge you to do so.

Mr. MASSARO. Thank you very much. Kristin, please.

Ms. REIF. Okay, thank you. I'm Kristin Reif from Philip Morris International. I'm the director of Illicit Trade Prevention for us, based here in Washington, DC. I want to thank everybody for their comments so far, and folks on the panel as well as the guests.

Illicit trade in tobacco has actually been labeled by the U.S. State Department as a threat to national security. There was a report issued under the leadership of David Luna, who's here today, that said as much. And right now the State Department is leading an interagency effort to come up with an international strategy in combating this, so we are looking forward to seeing the results of that.

For those who don't know, illicit trade in tobacco, the value of it on the low end is $40 billion to $50 billion a year. That's more than blood diamonds, oil, wildlife, and antiquities trafficking combined. So this is an incredibly serious issue. So thank you to the Helsinki Commission, especially Chairman Wicker and all of his staff there for bringing this together. They also led the charge last summer, holding a hearing specifically on this issue to show that level of seriousness.

I have a couple of questions, and I'll just read them through and then hand them over. The first one to Russ, when he talked about threat financing, specifically mentioning ISIS—I wanted to point out also that ISIS has made millions of dollars over the years trafficking in illicit cigarettes via confiscations and then resale of that product. The fines were for consumers and then taxing of safe passage through there. And I'm just sharing that as an example because, as a brand owner, and as someone who works in the illicit trade space, we often talk to law enforcement and intelligence services, and they tell us we don't care about the product; we're product agnostic. We care about the network. And I couldn't agree more. The point that I would be curious about, though, is if we all have an individual piece in filling the picture of how the network is gaining their money, what is the systematic approach for the U.S. Government to engage with us? Not just so we can protect our own markets and our own brands, but so that you all can have the benefit of that knowledge, whether it's the modus operandi, whether it's the hot spots of activity, under- and over-valuation of the product—I think we bring a lot to the table.

So my question to you—and I also have one for Christa as well—the question to you is—what can systematically be put in place—because a couple of people have talked about some of this informal sharing, and picking up the phone, and certainly a lot of people in this room get things done that way, but what can systematically be put in place?

A question to Christa—and I'm glad there is wonderful OECD representation here. I think that they've made wonderful, not only awareness raising, but also recommendations on free-trade zones.

To be clear, those free-trade zones in Panama end up flooding the Central American countries with illicit markets, illicit products that then go in the hands of MS–13 and others, and that is directly what is leading to people being on our borders. In the United Arab Emirates [UAE], the free-trade zones are exploited and product goes through Iran, and it goes to the Afghanistan-Pakistan border. That was in that State Department report, and the Department of Defense has listed it as a threat to national security as well.

So I am very appreciative of OECD leadership, U.K. leadership on this. What is the U.S. Government willing to do and recommend to our friends and allies—Panama is an ally; UAE is an ally—that they can be doing, because I think we have some common-sense, due-diligence measures that we are willing to offer, and is the U.S. Government willing to get behind those?

And then last, to Aaron, just really quickly—as I have stated my case about illicit trade in tobacco funding nefarious activity, it was recently reported on that alcohol and tobacco enforcement will be actually spun out ATF and go strictly to the tobacco tax bureau, taking a threat financing mechanism away from those with criminal investigations institutional knowledge and authorities and putting it in the tobacco tax bureau.

I don't know if you can speak to the rationale behind that and maybe what could or should be done about it.

Thank you.

Mr. MASSARO. Thanks so much, Kristin. We're going to start with your question for Russ.

Mr. TRAVERS. Yes, first to your point about illicit tobacco in particular, my listing of the ways in which ISIS was making money was not in any way meant to be—there are a ton. I mean, these guys are very entrepreneurial in terms of how they move commodities.

Second, unfortunately I don't have an answer for you other than to say that it was directed this last year. Treasury has stood up an interagency effort that is looking at threat finance. What I don't know is the extent to which they outreach to the private sector, but if you want to give me your card, I can certainly get you the [information ?].

Mr. MASSARO. Christa?

Ms. BRZOZOWSKI. Thank you. So if I understood the question, it's more on the foreign-trade zones than the free-trade zones and our relationships. So I'll narrow it to a couple of things. Again, as Chris and as I mentioned before, we are very much looking forward to the OECD report on the guidelines, your contribution, your steers on whether we are hitting that message right in the guidelines document would be great.

And then, absolutely, the U.S. did endorse that document in its draft stage, and unless it changes wholesale, we look forward to continuing to endorse it, and we take that forward to all our engagement with partners.

The link between—and I'll be brief on this—the economic prosperity and reduced migration flows is not lost on DHS and not lost on the interagency. To the extent that we, DHS, and the broader U.S. Government can make the situation in Central America, the Northern Triangle more secure, more safe, and more economically viable for people to enjoy their local area, I think we could all see the benefits of that.

I hadn't really thought about the more attenuated Panama to Central America demarcation, that circle, so that's an interesting takeaway for me.

Mr. SERES. And on your question regarding the removal of authorities, to speak on behalf of another agency that maybe has a different authority than we do, and it's not an area of expertise that I have. So it's something I can get back to you if we do have an FBI—[inaudible]—that's relevant. I'll get back to you later.

Mr. MASSARO. Lisa, please.

Ms. DYER. I just wanted to add that the United States Trade Representative puts together a report to Congress called the Special 301 Report, and for those who don't know, it's the countries that are not respecting intellectual property and are putting up market access barriers to those who own intellectual property.

The UAE was placed back on that list this year for some of the very reasons that you articulated, so just as an additional——

Mr. MASSARO. Thanks, Lisa. Thanks, Kristin. David, please.

Mr. LYNCH. Hi, my name is David Lynch from Sayari Analytics. We are a financial intelligence firm based here in D.C. that works with government, law firms and private sector to better map and track transnational illicit networks across a range of different threat verticals from terror financing to illicit trade.

As an organization, we leverage official public records across the globe with a focus on data sets that are traditionally siloed within a certain jurisdiction, within a language, or within a certain medium of dissemination. We try to bridge those gaps between jurisdictions and between languages to paint a hopefully clearer picture of the full extent of these illicit networks.

And so my question to you guys would be, for your respective mandates on illicit trade, what do you guys feel is your biggest data gap in trying to tackle these issues?

Mr. MASSARO. One for everyone.

Mr. LYNCH. Yes.

Mr. MASSARO. All right, so Lisa.

Ms. DYER. Interesting question. From a policy standpoint, from a persuading-foreign-governments standpoint, I think we have a lot of data that, at that very strategic level that we are communicating with, I think works. The statistics are compelling, they are powerful, it's a message that we're able to deliver that these actual illicit trade activities are harming your economy. That would be my answer to your question because we are talking at such a very strategic level. But others with a more tactical mission might have a different answer.

Mr. MASSARO. I was going to say, specifically how harm is occurring. How——

Ms. DYER. Yes.

Mr. TRAVERS. We could talk for hours. Ten years ago, Mike Hayden was talking volume and the velocity of data, and to Lisa's point, we are all drowning in it. I used to keep statistics on how much was incoming to NCTC every day. I've long since quit because there is so much.

The specific point you made with respect to financial data I agree with entirely. It's not just between and amongst countries, frankly. There are a host of legal policies, security, privacy reasons—we have these same challenges within the USG—and then when you are looking at financial, in particular, I've had many conversations with the big banks who would argue, I think, that the government has the context, but the private sector has the data, so how do you bring that marriage together in a way that doesn't give competitive advantage to one over another, and how do you respect the privacy rights.

I am an intel officer. How much U.S. persons' data do you or don't you want me to have? These are questions that we have not yet resolved as a country, and it just so happens that the financial datasets bring an additional level of complexity over and beyond—[inaudible].

Ms. BRZOZOWSKI. Great, yes, I should have gone first because I had an answer right out of the gate for you. So a little bit more specific, but on Lisa's flow of her—of the threats in the space—I would specifically say that we've got a pretty big gap that work in the OECD is looking to address, but any additional help or hands on deck would be appreciated on what are the new threats in the ecommerce space, and I think there is a particular interest in answering the question of whether we are seeing more counterfeit products or just the same number or volume, I guess, in different forms. So instead of coming in a giant container, there is now just as many counterfeits which are coming through all these kind of little e-packets. Answering that question is really necessary for us to, as I said, apply the right policy answers. And we just don't have a sense of that.

There's a particular interest as well in what we're terming low-value shipments, and low value because they tend to be not required to pay certain duties and taxes if they're under a certain threshold of value.

Is that value—is that waiver of taxes and fees being exploited by folks by either undervaluing the product inappropriately and/or by assuming or perceiving there to be a lighter law enforcement touch for those types of products? So very quickly the counterfeit threat in low-value ecommerce space.

Mr. SERES. And I would just like to add a comment from more of a tactical law enforcement perspective as it relates to intellectual property rights crimes and illicit trade.

From a law enforcement standpoint, we're just looking for information so we can try to identify where the bad actor is coming from—are they aggregating, is it a network, is it an organized group or is it just one guy, right? So how do we best place our assets from that perspective against whatever criminal group is out there?

That being said, I think a good comparison was made in regards to the banking industry. We've been receiving information from finance institutions for a long time. We've set up mechanisms, teams, and data information systems to cull that data, look for commonalities—commonalities of address, the bad guys—so we can target our effectiveness with our resource utilization.

Similarly here, we have bad actors who I think are agnostic to what platform they are going to utilize, whether it be one company or the next, one shipping lane or the next. I don't think they really care about that, so to the extent that we're seeing a bad actor in a certain platform, an ability to start to find a way to share some of that information, whether it's a bad IP address, a bad overseas address, et cetera, in an aggregated way so we can start targeting our resources a little bit more effectively, I think would be a helpful tool from a law enforcement perspective.

Thank you.

Mr. MASSARO. Thank you so much. START, please.

Mr. SIN. Good afternoon. Thank you very much for your participation and words of wisdom this afternoon.

My name is Steve Sin. I'm from START National Consortium based at the University of Maryland. I'm currently the director of unconventional weapons and technology for that organization.

Some of the work that we do—we have looked at emerging technology. I'm a radiological and nuclear terrorism specialist, so we looked at things like what kind of tech-

nology 5 or 10 years out from now will affect nuclear or radiologic terrorism in the—[inaudible]—space.

So my question from that perspective was, are there works or organizations or committees that you have that look at what illicit trade or what illicit trafficking would look like 5, 10, 15 years from now? Kind of do a net assessment—[inaudible]—we do, and that would be one of the questions.

And the second question actually is a personal question, just because I'm from academia. We talk about illicit trade and illicit trafficking, ordinarily, a lot of times we talk about it in terms of industry. So the question that I would have is, are there any efforts being done to limit—since our product is largely intellectual property—limit the trafficking of academic intellectual property so that we actually don't lose—because universities are a number-one target of foreign [governments ?] as well, especially universities like the University of Maryland. So I was wondering if there was a measure or something that is being done to address that, or do you need our help to be more involved. So those are my questions.

Mr. MASSARO. Is there anyone in particular you would like to address your questions to?

Mr. SIN. No.

Mr. MASSARO. Okay. All right. Anyone like to take it first? Illicit trade in 10, 15 years.

Ms. BRZOZOWSKI. I'll jump on that part——

Mr. MASSARO. Sure.

Ms. BRZOZOWSKI. ——very quickly. Just taking the fact that what came to my head immediately, and maybe the gut reaction is the best thing, or maybe you primed the pump by talking about emerging technology initially, but I do think that much interagency, and the White House, and administration, and congressional branch discussion on the new threats that we are going to potentially see with the emerging technology and—links to our ability to protect intellectual property. You see this in a Defense Intelligence Agency legislation currently under consideration, and which partners—or part of the new CFIUS, or Committee on Foreign Investment in the United States' modernization rules that have now added an export control component, and that link is that we've got valuable IP on emerging technologies that's absolutely critical to DoD, to DHS for Homeland Security enterprises, for Commerce, for some of the economic applications.

And the current export control regime might not be appropriately situated to account for these new emerging technologies. And we are kind of seeing vulnerabilities kind coming at different angles. The ability to export these might not be appropriately controlled, and we're looking just to take that up, but we're also seeing foreign acquirers just come in and wholesale buy the business or hire the engineer, and that's where this new legislation is looking to come at it from a couple of different angles.

When we're talking illicit trade, it's getting around some of these new tools and new requirements that the administration is putting in place.

Mr. MASSARO. Aaron, do you have——

Mr. SERES. Yes, I would just say, in regards to the academic property, I don't know of a specific initiative or effort in relation to that specific area, but it's something I'd be happy to put you in contact with the FBI's center and maybe discuss it a little further. I appreciate the suggestion.

Mr. MASSARO. Okay, yes, we'll move on to TraCCC, please.

Ms. KINNARD. My name is Kasey Kinnard, and I'm from the Terrorism, Transnational Crime and Corruption Center at George Mason University, and conveniently put academia together because that's where most of my comments lie.

We've been very privileged to work with a lot of the folks and organizations in the room, so I have several comments. I'll try to keep them concise.

Mr. Travers spoke about the difficulty of sharing information, but I wanted to specifically encourage everyone to continue to try and do that. And, specifically, we've heard a lot about including private industry in that. I would throw academia in the ring wholeheartedly, for several reasons. First of all, I would say that it helps to think about some of these problems more creatively, particularly when coming to a lot of—you've all spoken about intellectual property crime or terrorism. Some of those are crimes that are higher risk, and we looked at sometimes problems that are lower risk and therefore are a good, creative way to get at a criminal element, but you might have influence or get information from folks like academia.

Within academia, new threats is a place that we focus and would be a great place to help, hopefully, inform the executive which might also serve other purposes. When we talk about other governments and where you share information, we find sometimes that we might be more affordable than government researchers. We might also be able to get into a niche where the U.S. Government is not so welcome, and that has helped to make, create some bridges.

So I would also say that when getting into grants and programs, like most of the agencies do because we've gotten these funds before, will allow for some flexibility because academia tends to be able to be flexible, like transnational organized criminal groups are, but the U.S. Government is not set up to be. We can be flexible, but we've also been hindered when asked, by global partners, can you help us with this issue. Nope, I'm only a stovepipe. But we look at all illicit trade, and we know we are connected and we could help, but we can't touch it. So I would encourage that type of flexibility.

I also was encouraged to hear that money is moving a bit out of the absolute concentration of terrorism and into a bit of a broader spectrum because we've been saying for a long time we need to be looking at a crime-terror nexus. Crime is often the funding for terrorism, and we have found that sometimes getting funding—it's hung up unless you can point at a terrorism connection, which has been problematic because, to get that funding, some people have needed those connections and are not quite there.

We want the government to have the best and most academically sound information, but if you are hamstrung in trying to get that funding—[inaudible]—for getting the best information.

Thank you very much.

Mr. MASSARO. Thank you. We'll just go on to the next speaker, please. Cyndi [sp].

Ms. BRADDON. Thank you. I am here today for a new organization called Trace It, and only been around since last September, and essentially, and it's an organization that consists of business, companies that are cross-sector—we represent 11 sectors and everything from alcohol, to pharmaceutical, to oil and gas, to tobacco, to counterfeit goods, wildlife, forestry, et cetera, and also concerned with human trafficking.

As an entity, we were formed basically to try to unite, across sectors, businesses to come together to advocate on behalf—or to create a voice of advocacy, working with governments around the world to deal with the issues of trade.

One of our first products, which Chris mentioned, was that we commissioned the Economist Intelligence Unit to prepare a global, illicit trade environment in-depth, and it analyzes 84 countries which represent 95 percent of GDP, 95 percent of trade, and it measures how each of the countries stand up and how they are—through policy primarily—set up to either encourage or discourage illicit trade.

We did this because we wanted to expand the learning around what are the better practices, so we can go to governments and help advise them on where efforts need to be made. And what we learned through the process is, to quote Chris again—is that everybody needs to pull up their socks a bit, including us here in the United States.

We also did a case—a report on free-trade zones, and picking up points that have been raised before, and what we did was put together five cases studies, including in Panama, and really identified some areas that need work—most commonly is devoting more resources to hiring and training, customs and law enforcement to work together and to do their jobs and to do it with due diligence. And what we'd like to see is more coordination—more formal coordination between the private sector and all stakeholders, and government, to help stop illicit trade.

So let me start with a question, and that is with regards to free-trade zones. And maybe it's from State and Homeland Security across the board. What do you envision will change in the near future that can continue to facilitate trade—the good trade—but can help with stemming the really serious issues we have with illicit goods going through either small packages or large containers?

And second, knowing that China and Panama are negotiating a treaty now, with regards to what we got to see in Panama, what's the U.S. Government doing to 3:13—[inaudible]—that especially?

Mr. MASSARO. Great, thanks so much. Shall we start with Christine—Christa? [Laughter.] You're up.

Ms. BRZOZOWSKI. All right. I will probably speak to more of the—well, first let me thank you for the excellent work on the index. I mean, that's exactly the kind of data that's really necessary to help us as DHS, as the U.S. Government, and then in international forums, like the OECD terror and illicit trade task force, to understand what's working, what's not, and to be able to identify best practices that can then be promulgated in various ways.

I'd very much love to—and I'm assuming it's just online, but I'd love the case study on Panama that you just did. This is a fairly new issue to me, but as I said, we are exploring ways, in concert with the development bank, and USAID, and of course, State Department, on how a security and prosperity message supporting Central American and Northern Triangle countries in a variety of ways to reap those benefits. So we'd love to see that report.

On the China-Panama free-trade agreement, I don't have anything on that. This is not my area, about what the United States is probably doing. If I knew, I probably couldn't say, so—[laughter]—I'll just hit quiet and mute on this one. [Laughter.]

Ms. DYER. I will say that it's not just Panama that people are concerned about where China is expanding, and not just within the free-trade zone. Africa is a huge area, and

I think there's a lot to watch there and keep an eye on how we do keep the good stuff coming and the bad stuff not.

I will actually take your question back to some of our free-trade-zone experts, and I'd love to take a card to—[inaudible]—with me.

Thank you.

Mr. MASSARO. Megan, please.

Ms. GIBLIN. Megan Giblin of the U.S. Council for International Business. I am the director of customs and trade facilitation, and unlike Christa, I am steeped in the details, mostly. [Laughter.] And unfortunately, I could probably talk to you about classification codes, and valuation. And Susan, thank you for your mention about USCIB being the—[inaudible]—unfortunate that my boss is the chair of the trade committee, so, feel free to reach out if you have any questions.

And I just wanted to make a couple of points, to add some discussion to discussion points from earlier, so after Jerry's point about data elements, and sharing customs data with other governments and other government agencies, I know from our membership perspective, for a number of reasons over the past year or so, we've talked about concerns about data being shared with other parties, under what mechanisms, and unintended consequences of that information being shared as a result of questions about trading, do others know what they are looking at, or potentially controls around that data, and so that's the discussion that we are having with some of Christa's colleagues.

And then I just wanted to touch on Rob's point, and at a much more granular level, so in the context of the Customs operational advisory committee, there is a group looking at—at least in the customs space—emerging technologies—[just wanted to leave that there ?]—so it's a subject matter—[inaudible].

And then back to Christa's point about the work going on in Brussels and the international discussions—again, being steeped in the content details like—[inaudible]—there has been discussion and context about looking at emerging technologies,—I just thought that would be helpful for you to understand.

Thank you.

Mr. MASSARO. Definitely, definitely. Thank you so much.

Now, Crawford, I know you've been waiting very patiently. [Laughter.] I saw you were the first to flip it and then had to wait 2 hours to speak, so I really——

Mr. ALLEN. This is called the last——

Mr. MASSARO. I really, really appreciate it. [Laughter.] Thank you so much.

Mr. ALLEN. The last man caught standing. [Laughter.]

So thank you very much. My name is Crawford Allan. I'm a senior director of the TRAFFIC group at the World Wildlife Fund, and we've been working on setting up the first global coalition to end online wildlife trafficking. And we've got 22 of the world's biggest companies involved—[inaudible]—Google, Facebook, Microsoft, Instagram. We've got 10 Chinese companies—Alibaba, Tencent and Baidu—all working together to prevent this pernicious threat of trafficking in wildlife.

One thing we have learned in this is that there are some really critical nexus here between the companies, the online marketplaces, between the parcel companies, the express courier companies, and between the paying and processing companies in the finance sector. What we are finding is we don't know how to bring those three sectors

of finance, transport, and commerce together, and we wondered whether people around this table or our lovely panelists here had suggestions or recommendations about that, because we feel this is a trick and what we are missing is bringing those together, and we think that they've all got a piece of the puzzle, but they're sitting there and doing it separately. And I'm sure that many of you have been through hoops of working in the private sector yourselves, for your own interests, that we have still yet to learn, and we would love to learn more.

I also think the other thing that we've found very much is that it's absolutely critical, and what you all say is true—information sharing is the one blockage that we find is most pertinent and most problematic. We know that we've got a fortunate situation where hundreds are sitting together and sharing best practice. How do you—[inaudible]—tech companies, they are really [competitive ?] with each other, but around this issue of wildlife they put that competition aside and they are really trying to share information about how we refine algorithms to protect wildlife, how we prevent the odds of being poached in the first place. I'm sure you've got expertise and insight that we could learn.

But what platform, what forum could we take this expertise and join these people together? We're all from different sectors. We're from probably the best—[inaudible]—in the world, which I'm going to—[inaudible]—[laughter]—take them to pharmacies to give them the cigarettes. How—what platform is it—[inaudible]—that could bring us together to look at the interface between online, transport, and payment—and finance. I think you've probably got some great ideas about that, so I really appreciate it. We just need to build trust with these companies. They're very scared of working with law enforcement, unfortunately, in sharing information.

Thank you.

Mr. MASSARO. Would someone like to start with that? I assume—[inaudible]—that the right person will start.

Ms. BRZOZOWSKI. Yes, welcome to my world here. [Laughter.] That very question, that, very powerful, very economically successful companies, different agendas, different perspectives. People are realizing that things are changing, but maybe not—without being able to control where they're going, aren't jumping up and down to say, come regulate us, U.S. Government and other government. [Laughter.] So surprising. But those are exactly the types of groups that we're trying to, as an interagency—have engagement with and understand from the U.S. perspective where we see ourselves—what concepts need to be tested, and where we see ourselves potentially in 2 to 5 years.

This is exactly—I'll put in a pitch—this is exactly the conversation that is happening in Brussels, as I said, today. It's the World Customs Organization ecommerce working group. It's from a very specific Customs perspective, and we would like to keep it like that. So that's one forum, I think, for some of these engagements. I believe they will be getting a mandate to extend their working group for another year, and we're looking right now to figure out how to organize that so that that year is beneficial, so that we get some standards coming out of that year, we get some definitions coming out of that year. We'll maybe get some additional case studies out of that year. So now is the time for engagement with that group.

And then Chris and I, following David's lead, hosted the Countering Illicit Trade Task Force within the OECD, so a different group of stakeholders, but in some ways a good set of stakeholders will be taking on this issue. We're working now to figure out what

our next-year and 2-year trajectory looks like, what workshops are necessary on what issues. I think we've got general consensus among the member States that we do want to tackle e-commerce next. That's a pretty big mandate; almost as big as how do you solve illicit trade. [Laughter.] So defining that work plan and coming up with that schedule of the who needs to meet around what issues in the coming year, 18-month timeframe. But very, very timely, again. I don't have the answer yet, necessarily, but we'd love to engage to make sure you're part of the development of the answer.

Mr. MASSARO. Lisa, you wanted to say something?

Ms. DYER. I'll just add, in addition to what Christa has said, that our team has worked with the International AntiCounterfeiting Coalition to put together a toxics/counterfeits workshop. And the idea is pulling together people from different sectors around to look at what hidden dangers are in some of our most common consumer items, such as luxury goods, cosmetics, toys, apparel, and test them for those toxins, and to see what exactly are we finding that could then be used for a public-awareness campaign to get some more information out to the public to support consumer safety.

I will take your suggestion back to the team in the State Department that works on wildlife activities, and—[inaudible]—similar things.

Mr. MASSARO. And IACC is here, right? Over there? Great. Cool.

Jim?

Mr. DUGGAN. Hi. Jim Duggan from Coty, fragrance and cosmetics. Lisa just stole what I was going to say.

Ms. DYER. I'm sorry. [Laughter.]

Mr. DUGGAN. So I'll start in reverse, then. Aaron made a very excellent point. Arrests are a significant way to curtail, but you can't arrest your way out of this. And I've heard that ever since I've been—[inaudible]—counterfeit for the last 18 years. It's been stated by many other federal agents that I've worked with over time. Homeland Security, Customs and Border Patrol, and the IPR Center are all excellent tools for us to use to combat the problem.

At the end of the day, the most important thing from my perspective is educating the American consumer. When I talk to the American consumer in a counterfeit 80 to 90 percent of the time I get a shrug of the shoulder; what's the big deal? And they just don't get it, and they don't understand it because at the end of the day, the consumer wants—and it's not just the American consumer—it's my knowledge of the world that every consumer wants to get the product at the best price.

So we are working with Joe Giblin [ph], under his group, and we're very happy to be—further, that the company is very interested in seeing that through.

Ms. DYER. Thank you for investing the time.

DUGGAN: Education is effective, just so important. If the consumer is not there—the consumer doesn't buy it, that world is going to dry up.

Mr. MASSARO. There has to be demand for these products.

Ms. BRZOZOWSKI. Can I——

Mr. MASSARO. Yes, please.

Ms. BRZOZOWSKI. Yes, I thought of—thank you for that comment. A very quick note on that, and I think it's a great example of why the data is going to be so critical to us. I'll go back again to this in-country, in-depth study the U.K. did utilizing the OECD,

which found that, I think—I'm trying to look through my stack here—about 50 percent of consumers said they weren't aware that they were buying a counterfeit product, so that gives policymakers an immediate, okay, now half the problem is people that do know they're doing it, and we've got to dissuade them through campaigns at the State Department, but we've got half of these people that don't even know that they're doing it, so that's a whole set of policy options to counter it.

So that was an eye-opener for me when I read that report, and we're very interested in trying to get that type of granularity for the U.S. market as well.

Mr. MASSARO. Okay, do we have any other questions? We've got maybe time for one more if anybody's got something to say.

All right, so we're all exhausted. That's fantastic. [Laughter.]

So thank you all so much for coming. I want to thank our panel of executive branch officials, if you will join me in a round of applause. [Applause.]

And to all of you, as well, I just want to extend my sincerest thanks, and on behalf of our, again, bipartisan and bicameral leadership, I can't think of a single member, a single commissioner who doesn't care deeply about these issues. I really hope that we'll keep this dialog going. And thank you all again for attending.

Mr. LUNA. Paul, would it be possible to circulate the contact information for people who attended the hearing?

Mr. MASSARO. Sure. Anybody object to that? [Pause.] No? All right, great. We'll do it.

[Whereupon, at 3:52 p.m., the roundtable was adjourned.]

○

This is an official publication of the **Commission on Security and Cooperation in Europe.**

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe [OSCE].

★ ★ ★



★ ★ ★

**www.csce.gov** **@HelsinkiComm**

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.