FPOV
FUTURE POINT OF VIEW

Blacklisting Our Future

A WHITEPAPER DISCUSSING THE IMPACTS OF AND POTENTIAL ALTERNATIVES TO THE PATH OF DIGITAL NATIONALISM RECENTLY ADOPTED IN THE U.S.

Scott Klososky
Founding Partner of Future Point of View, LLC.

TABLE OF CONTENTS

THE PURPOSE OF THIS WHITEPAPER

Every long form document should have a clear purpose, so that the reader understands the reason for its length. It is my intention to be respectful of your mental attention because it is valuable, and I do not want to waste it. For that reason, I want my objective to be clear.

The singular goal of this document is to help legislators and the public gain a clear understanding of two potential futures. One is a future in which the U.S. attempts to solve cybersecurity issues by blacklisting foreign companies without a clear set of guidelines. An alternative future is one where the U.S. takes on an international leadership position by using new techniques and processes to provide a higher level of security for the U.S. and any other country who chooses to participate with these new processes.

These two futures would be dramatically different in their impact on the U.S. economically as well as in the ability for the U.S. to create a secure landscape for its organizations to grow and flourish internationally. Given the sophistication of the malicious actors in cyberspace and the evolving threat landscape, it is important for all countries to develop an objective and transparent basis for knowing which products and services are worthy of trust. Absent this ability, digital threats will continue to grow, or at the other end of the spectrum, countries will choose to isolate for digital security and that comes with its own dire consequences. There is a larger picture to be addressed than the dangers of Chinese companies providing telecom equipment in the U.S. and other Western countries. This is simply one example of the need for the global community to ramp up security and conformance.

The United States has always enjoyed the comforts of being a world leader when it comes to selling technology internationally. Therefore, the steps taken by the U.S government over the past four years might appear to make sense on the surface. However, when played out over a period of time, the U.S. will see the growth of digital nationalism. Continuing down this path will not end well because it will cause collateral damage that is seemingly not understood by our leaders today. The collateral damage the U.S will face because of these policies is outlined throughout this document.

It is our sincere desire that you consider the background information and the four alternatives provided so that our country is not painted into a corner we will regret later after it is too late to reverse.

THE DEFINITION OF DIGITAL NATIONALISM

We have a problem worldwide, and specifically in the U.S. with cyberwarfare and cybercrime. U.S. companies and organizations are in many cases large, wealthy and innovation leaders. This makes them prime targets for attack by cyber criminals and government sponsored cyber terrorists. At the macro level, our country wide voting system was even a target because the influence we have in the world. We need to build stronger defenses. We also need to be very thoughtful about using defensive tactics that will cause more long-term economic damage than the present risks themselves. We are blacklisting international technology providers and partners from the U.S. market based on concerns centered around possible cybersecurity impacts or data privacy breeches. The strategies enacted by the federal government over the past three years seem to be politically driven brute force moves that are more harmful than protective of the U.S.

Erecting a digital wall haphazardly might provide good political soundbites and play well to a constituency that does not understand international dynamics. However, it does precious little to address U.S. cybersecurity concerns much less large international problems.

At worst, the blacklisting of international companies based more on their country of origin than evaluating risks against a well thought out model creates a false sense of security that will actually do more harm than good as cyber-attacks and breaches continue to mount daily, impacting huge companies as well as government. We need better solutions, and we have them available to us.

Let's take a step back and examine the history around technology collaboration on an international scale and how we have addressed problems in the past.

Years before the internet, all countries agreed that having an international telephone system was a great idea. In order to execute on this concept, there had to be standards in place in order to allow a voice from one place to be transported across wires (and countries) to a different place. Countries had autonomy over the specific numbering schema in which to identify a person or place within its borders. Even this autonomy, however, had limits.

Countries had to adhere to a few basics so switching equipment could be built in order to route calls thousands of miles and have them accurately ring where desired. Over decades, leaders everywhere learned to agree to collaborate with the manufacturers building equipment and the organizations tasked with handling the business of providing telephone services in country.

Depending on the political system in place, telephones were either looked at as a wonderful tool of convenience, connection and freedom, or a possible danger to power because they freed people to talk to whoever they wanted to, whenever they wanted to. Laws were put in place differently around the world to control the privacy of telephone conversations.

There is a saying, "history does not exactly repeat itself, but it often rhymes." Politics, privacy, and control are constantly changing to this day as we have recently seen with big tech deleting accounts based on their beliefs about community safety. Control of verbal conversations has now been supplanted by control of data flow and digital conversations. Differing laws around the world make it challenging to understand where lines should be drawn for a healthy society.

In the past, some countries put up virtual telecommunication walls so calls could not be completed outside the country or routed to specific countries. It took decades for some of these walls to come down. Today we wrestle with the free or controlled flow of data and information and the new dynamic is the high level of digital crime that is coming with open digital borders.

The internet came later, and in much the same way, leaders and countries all over the world decided they wanted to participate in the World Wide Web. This took even more collaboration because to deliver internet access, in all of its forms, is a lot more complicated than the telephone system.

As open as the internet has been, there have been some countries that have chosen to block content at its borders, to isolate people, and to only allow citizens access to content approved by that country's leadership. In the free world, we look down upon regimes who try to control access to information by neutering the free and open internet. This has proven to provide no security for their people from cybercrime or data theft, and the motivation is again, control of power.

We see a restricted internet as a denial of a basic human right. This is a form of digital nationalism, but in this case, the only toll is on the users in that country who are denied the informational freedom an open internet can provide. We will be discussing a different version of digital nationalism in this paper. That is the blocking of foreign technology companies from access to the U.S. market, or the banning of U.S. companies from selling their technology innovations on the world market.

Digital Nationalism:

The blocking of foreign technology companies from access to the U.S. market, or the banning of U.S. companies from selling their technology innovations on the world market.

BLACKLISTING OUR FUTURE

While we agree there are situations where foreign companies may deserve to be blacklisted, we do not agree that doing this without clear guidelines, evidence, and due process since this is what our countries legal process is based on. Governments can say publicly they have so-called “evidence” but not disclose it under the “national security” umbrella. Due process through the justice system is appropriate if we aspire to be the “rule of law” country.

It could be argued that the U.S. has discovered a healthy balance of using telecommunication systems in a way that provides freedom for citizens while also giving law enforcement methods for surveillance when evidence is warranted.

Conversely, the current version of U.S. digital nationalism is a poor example to set for the rest of the world when we hold ourselves out to be great examples of freedom. We are banning foreign vendors without clear rules or evidence as to the issues we are seeking to solve.

The reality is the world has made economic and lifestyle progress by having an open internet that supports global economies, information sharing, and free communications. The U.S. was one of the originators of the Web and instead of supporting the original ideals that made it successful, we are now taking small steps backward instead of moving forward to deal with the specific problems of cybersecurity we and the world are not facing.

"We are very disappointed. The United States, the country that funded the early development of the Internet, is now considering policies that would fracture it into pieces. This is part of a larger disturbing trend where governments directly interfere with the Internet, attempting to score short-term political points without regard to the long-term damage that results." *// INTERNET SOCIETY*

To be sure, cybercrime has become a plague on the free and open use of the Web. Today, even free nations are wondering if they need to control access to the Internet as well as the tools and applications that allow us to access it.

Along with cybercrime, user data privacy is also a serious issue. Billions of users worldwide have become comfortable installing applications to their digital devices without understanding the data they may be sharing – and who they may be sharing it with.

The European Union provided a good start to improving the data privacy model with GDPR. What we really need are global rules and practices with accountability for nonconformance with data and network privacy rules.

U.S. companies like Google, Twitter and Facebook when examined through the lens of other countries, might appear much worse from a security and data privacy standpoint than Chinese companies look to us today. In other words, a person's perceived security and data privacy risks have a lot to do with their country of origin and perspective.

Clearly there are risks and concerns that need to be dealt with when it comes to internet access and tools. We had years to figure out how to maintain an international telephone system that connected billions of people around the world. Although countries built their own systems in their own styles, we found ways to integrate these systems for the good of users. The internet must be the same. However, we must also avoid slipping into digital nationalism in which we restrict free trade and innovation without well stated guidelines for companies and countries to follow.

Free trade has always had benefits for consumers and suppliers. Unfairly restricting trade lowers competition and artificially boosts pricing to consumers. Restricted technology will hurt consumers, manufacturers and the U.S. economy for years to come if we do not move to wiser options to provide national security and data privacy.

"In reality, banning is more likely to increase — not reduce — risk, because it builds up distrust among countries and companies. Other countries may retaliate by banning U.S. companies and the situation could rapidly spiral. The abuse of 'national security threat' is snowballing and leading to an escalating trade war that could disrupt world trade.

"We saw a similar situation caused by the Smoot-Hawley Tariffs in the 1930s. The goal was to protect U.S. farmers and other industries that were suffering during the Great Depression by raising tariffs and discouraging import of products from other countries. But, not surprisingly, almost all of the U.S. trade partners retaliated and raised their tariffs. That resulted in U.S. imports decreasing 66% and exports decreasing 61% making the "Great Depression" much greater. In general, there are rarely winners in trade wars, and probably not in cyber trade wars." // HARVARD BUSINESS REVIEW

NATION-STATE CYBER CONFLIT AND CYBERCRIME

In order to evaluate the wisdom of building digital walls around the U.S. versus any other possible solution, we must understand why reasonable people argue for the need to blacklist technology related organizations from doing business in the U.S. or any other country we consider to be an ally. Let's start with the two big dangers we are seeking to avoid:

Nation-state Cyber Conflict is the weaponized use of technology by a nation state intent on causing harm to a competing nation, or gaining some operational, economic, or military advantage through digital subterfuge.

Cybercrime is sponsored by criminal's intent on enriching themselves monetarily at the expense of anyone they can abuse.

Both of these are dangerous, expensive and abusive to U.S. organizations and people. Both are growing in frequency because the practitioners are getting more sophisticated around the world. As mentioned earlier, the U.S. is a prime target for reasons such as, poor individual and corporate cyber hygiene, fractured Federal/State cyber and privacy laws and lagging legal and regulatory guidance (out of touch lawmakers). The U.S. government must play a role in doing whatever it can to protect its citizens and companies from cyber-attack in ways that make long-term sense.

There is a difficult reality in the security field in general. That is finding the best risk balance between internet access and security. We can make access to systems very difficult for digital criminals, but that also can make it difficult for a user as well. It is the same dynamic on a national basis. We can put up digital walls to keep other countries and their companies away from the U.S., but that will shut down a lot of our ability to be part of the world economy. The strategic question is how to best maximize national security without shutting down free market access to the internet from foreign countries or companies. We need to do more than try to outmuscle other countries' cyberwarfare teams, blacklist a few companies, and then act like we have a well-organized strategy.

"The U.S. government should push for multi-stakeholder efforts to develop common approaches to supply-chain diversification, to ensure an open and transparent international 5G standard-setting process, and to promote voluntary agreements on security standards. Regardless of whether Huawei is banned from building U.S. 5G network infrastructure, Chinese networks and Chinese equipment will be connecting to American networks, so the U.S. must take proactive steps to deal with this." *// LAWFARE*

“Eighty cybersecurity experts were asked about the Huawei ban. 61% said it won’t make the U.S. more secure…cybersecurity experts worry the ban will diminish U.S. influence over the security of new technologies.”

via “Trump’s ban on U.S. companies supplying Huawei will not make the country safer experts say.” - The Washington Post, June 4, 2019

THE EFFICACY OF THE U.S. DIGITAL BORDER

There is always a tension between freedom and control. From childhood, we struggle with parents who put rules in place to keep us safe. As children, we desire our parents to have less control over our lives because our aims are often at odds with theirs. We want total freedom, and our parents demand controlled freedom in order to keep us safe. Countries and their leaders are no different.

People generally want freedom to do as they please. However, leaders demand controls to either keep people safe, reduce chaos, or to assure a stranglehold on power. There is always such a fine line between control that serves a positive purpose and control that overreaches into the negative.

There are examples of having a digital border that makes sense, such as blocking traffic from known digital criminals or countries who support cyberwarfare targeting U.S. businesses. The Obama administration blocked Russian cybersecurity firm Kaspersky. The Trump administration took reasonable steps to block foreign technology companies from doing business in the U.S. when they were found to be engaging in activities that go against our democratic ideals, such as a number of military and surveillance companies in China.

Then we went too far. We began to blacklist companies like Huawei over concerns that their 5G equipment could be used to eavesdrop on information flowing over the telecom systems. Or, that Huawei could be convinced by the Chinese government to turn off systems that would impact the integrity of telecom service delivery in countries in disputes with the Chinese. We also sought to ban WeChat and TikTok use in the U.S. over concerns they are gathering user data in ways not disclosed or understood by users and that could provide advantages to the Chinese government. Again, it is reasonable for the U.S government to be concerned about the possibilities stated above, but why target these organizations and not others.

We are not the only country to become concerned with technology companies domiciled in China. Depending on political relationships with China, there is more or less proclivity to put a digital border in place, the European Union and Australia are examples as well. It would make sense to develop frameworks for security and data privacy that could be implemented worldwide, instead of every country trying to figure out which companies are additive to the world and which are abusive.

We are not debating that controls on companies doing business in the U.S. is unwise or that the U.S. government should allow uncontrolled freedom to every organization no matter what their standing or motivations might be. We are simply stating that the rules we are using today seem arbitrary and are not stated clearly for companies around the world to follow. We are also forcing other countries to compete with U.S. technology firms instead of being customers. In other words, our motives might sound good, but our methods are not wise long term.

"*The belief that the U.S. can build a digital wall against large international technology providers and not pay a heavy price is flawed. Isolating ourselves from selling and purchasing world class technology will only stunt our growth. When we restrict tech transfer for international companies, we drive them to compete with us and not only take away market share we would have had, but also take away markets we have been leaders in for years.Chris Finan, cybersecurity director on the National Security Council during the Obama administration who's now CEO of Manifold Technology, called the Huawei ban an 'act of self-immolation in the name of security" and argued it "will do nothing to change Huawei's or Chinese government behavior over the long term."*" *// THE WASHINGTON POST*

UNINTENDED CONSEQUENCES

Any major policy action taken by a country's leaders will have ramifications that reverberate throughout society, the economy and the constituency. To the extent possible, it is helpful to play out as far as we can the impacts of a new policy action just to assure it has the end results expected.

If we take the latest companies the government has worked to blacklist and play out the impacts, here are what the consequences will likely be:

Other countries are forced to invest in their own technology suppliers instead of buying U.S. products. This is one of the most dangerous long-term impacts. The semiconductor industry is a great example, because blocking them from selling to a large international company like Huawei forces them to find other suppliers or create the semiconductors on their own.

"China is accelerating its quest for technological self-sufficiency amid a tech trade war with the U.S. Chinese semiconductor companies have raised the equivalent of nearly $38 billion so far this year, more than double last year's total, according to S&P Global Market Intelligence. More than 50,000 Chinese companies have registered their businesses as related to semiconductors this year, a record that is four times the total from five years ago." *// WALL STREET JOURNAL*

A loss of U.S. technology jobs. By blocking our technologies from being sold to Chinese (or any other country's) companies, we push foreign companies to fill the gap. This will cost thousands of high paying jobs on our country that will never come back as long as we push international customers to find new suppliers.

"The ban will financially harm the thousands of Americans employed by the U.S. companies that do business with Huawei, which buys more than $11 billion in goods and services from U.S. companies each year. A total ban on Huawei equipment could eliminate tens of thousands of American jobs." *// NEW YORK TIMES*

Creates a dynamic where other countries come after U.S. manufacturers in a tit for tat situation. *Large U.S. companies like Apple, Google and IBM enjoy a good percentage of their revenues coming from other countries. The more we shut our digital borders to competition, the more they will respond in kind. This is the concern with the U.S. actions concerning TikTok. Forcing them to sell part of the company to U.S. firms in order to do business in the U.S. is setting up any other country doing the same to Apple or Facebook.*

"And China might retaliate with similar bans against U.S. technology "that ultimately stagnates our tech leadership around the world," Katie Moussouris, founder of Luta Security, warned. "The balkanization of software and hardware is a game the U.S. cannot win in the long run," she warned." *// THE WASHINGTON POST*

Restrictions of U.S. companies from participating in international standards bodies discussions if Huawei is present. This did nothing but cripple U.S. telecom equipment providers and purchasers from having any influence over standards – including security standards.

"At least the intention behind the ban was understandable: The U.S. government sees Huawei as a national security threat and wants to limit its growth, but the way the trade ban restricts the sharing of technology proposals in standards setting bodies only hurts U.S. firms—not Huawei." // INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

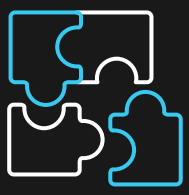
Robs U.S. companies of R&D money from international sales, and lowers our ability to compete. When U.S. companies lose revenue internationally, and are restricted from collaborating with foreign companies, it weakens their ability to invest heavily in research and development. This slowly allows companies from other parts of the world to build better technology and capture a market the U.S. company could have played in. For example, look what has happened with U.S. telecom equipment providers. We were once the most advanced in the world. Today we are not. So now that 5G is critical infrastructure improvement, we are going to lag other countries with its rollout and capabilities.

"This will only accelerate China's technological independence and end up impacting the U.S. economy longer term," // Mark Weatherford, a former Department of Homeland Security cybersecurity official who's now a global information security strategist at Booking Holdings.

In the end, we are not safer today than we were before we started blacklisting companies without a transparent framework for decisioning. The U.S. can ban companies believing we have done it righteously and they will often continue to expand and grow and take over market share that could have been earned by U.S. companies. That trade off will do more damage than if U.S. government chose to be leaders in building international coalitions to adopt security and data privacy frameworks that can help protect all countries andmake it unfeasible economically for a company to abuse the international rules.

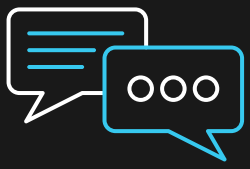
Unintended Consequences

BLACKLISTING OUR FUTURE



Other countries are forced to invest in their own technology suppliers instead of buying U.S. products.

A loss of U.S. technology jobs.



Restricts U.S. companies from participating in international standards bodies discussions if Huawei is present.

Creates a dynamic where other countries come after U.S. manufacturers in a tit for tat situation.

Robs U.S. companies of R&D money from international sales and lowers our ability to compete.

WORLDWIDE DIGITAL LEADERSHIP

The United States has had the opportunity to be leaders in the world with many aspects of technology. We have generated some of the world's largest and most well-known companies. U.S. organizations have pioneered many critical technologies, and often led the world in getting those technologies adopted by consumers for everyday use. We now have a chance to be worldwide leaders in the creation of new programs to help lower the risks from Nation-state cyberattacks and digital crime.

Our government leaders have an option today, and that is either to protect the U.S. individually or help put systems in place to create a safer, more secure cyberspace worldwide. An interesting example cited earlier of putting a well-organized framework in place to provide security protections is what happened when the EU put GDPR in place to protect European citizens from data privacy violations. GDPR applied to any company in the world that does business in the EU.

This provided clear direction for the rest of the world to either copy or ignore. The EU could have just banned companies they felt were predatory on EU citizens but instead, they put rules and penalties in place to assure good behavior in their countries.Interestingly, if the EU would have chosen to ban companies because of their data privacy concerns, they would gone after U.S. companies early in the process.

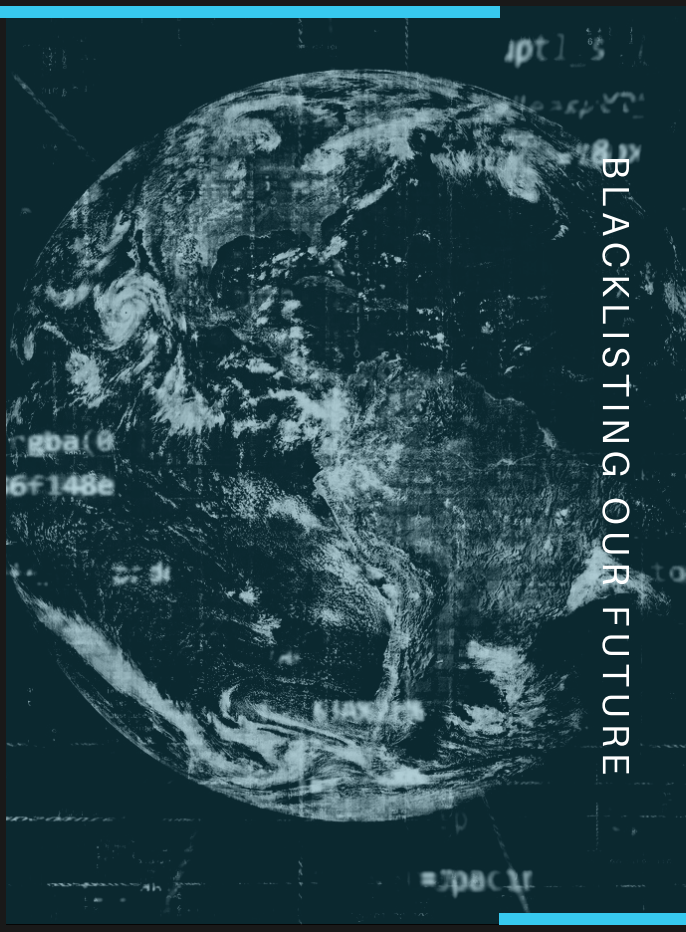
The U.S. can be a leader with cybersecurity in the world by supporting international frameworks, conformance programs, and independent testing that states clearly what is acceptable and not by companies doing business around the world. Regardless of the motivation for why they break the international security rules, they would pay a heavy price that would deter most of them.

The purpose of this paper is not to just point out a misstep in current policy, it is to provide better solutions. We will now provide four options that describe how the U.S. can be world leaders for a greater good. Some of these solutions could be combined so should not be looked at as exclusive to each other.

"Walling America off—whether physically, economically, or digitally—is expedient, but it is the ultimate self-defeating move for a 21st-century power that relies on international interconnectedness. By retreating behind its own borders, the U.S. risks subverting the only international approach to technology that can keep it safe and prosperous: an open world." // FORTUNE

“This will only accelerate China's technological independence and end up impacting the U.S. economy longer term,”

- Mark Weatherford, a former Department of Homeland Security cybersecurity official who’s now a global information security strategist at Booking Holdings.



ALTERNATIVE OPTION ONE

Required Domestic Manufacturing for international technology providers. The U.S. government could create legislation that creates clarity around the need to require a foreign technology supplier to have domestic locations to build or program systems. This would allow a much higher level of oversight to products being used in the U.S. by adding a new layer of security through "auditors or examiners" who randomly would inspect the products under this mandatory schedule.

The requirements for domestic production could be based on a scoring system that gives points for the level of criticality and trust for the systems the foreign organization supplies. This provides a very public and transparent system for allowing foreign technology companies to have access to the U.S. market. Aside from helping to provide a new layer of security, it also has very positive impacts on the U.S. economy because it creates jobs and keeps domain expertise in the country.

The scoring system could be based on the factors listed below:

Infrastructure Criticality Rating	*How critical is the product to some form of domestic infrastructure like utilities, telecom, construction, computing*
Prior Security Activity Rating	*Has the organization been found to break national security protocols in the past - anywhere in the world?*
Event Damage Impact Rating	*What is the potential damage to organizational and national security if the product is found to have security issues?*
Non-Visibility of IP Rating	*Can the technology IP imbedded in product be easily reached and tested?*
Stolen IP Usage Rating	*Does the company have a history of stealing IP to design and build their products? Does the product itself have stolen IP imbedded in it?*
Platform Integration Need Rating	*How critical is the product in supporting a domestic technology stack that will not work in a world class way without it?*
Country of Origin Rating	*In what country are the majority of the parts designed and manufactured now and is the company under the control of a nation that is actively using cyber warfare against the U.S.?*
Supply Chain Risk	*Possible interruptions to domestic operations and manufacturing supply chains*

If the score for the foreign supplier is high enough due to prior security violations and the criticality of their products/services, they could then be blacklisted by policy.

This model is equitable in that the same framework could be adopted by other countries which would put more pressure on international companies to be sure their products are trustworthy. It could also lead to more U.S. companies creating local manufacturing and development facilities if they are supplying critical technology and do not want to risk using international providers of key components.

The key thought is that a transparent and well documented framework of rules and guidelines would help all organizations, domestic or international, know the rules the U.S. feels necessary to provide security and data privacy, as opposed to uneven blacklisting as the only consequence available.

ALTERNATIVE OPTION TWO

Legislated Penalties on Companies who Deliver Exploiting Products. This is a direct analogy in cybersecurity for what GDPR is doing in the EU for data privacy. If the U.S. Government would pass legislation that creates clarity around what they find to be abusive cybersecurity tactics, we could then enforce substantial financial penalties against organizations that break what need to be very clearly stated and advertised rules. If the penalties are high enough, there would be no economic logic to take the risk of selling abusive products in the U.S. even if a company's government of origin demands it.

Articles would be documented that state clearly what is considered a violation of U.S. security policies. Any company that is complicit in violating a stated article would immediately be fined. If the violation is serious enough, the organization could then be blacklisted from doing any business in the U.S.

The model for the financial penalties would scale so the risk levels of what was abused get more painful as the possible impacts grow. The GDPR model was to levy maximum fines that were either a set number like $22 million USD, or a percentage of annual revenue. This model makes it very risky for a large company to abuse the rules because the fine would be very painful.

A positive dynamic of this model is that any of the fines that are levied can then be used to finance more enforcement so the risks of falling afoul of these regulations just don't make sense for any organization no matter how much pressure they come under from their government to attempt a cyber breach technique in the U.S.

"Policy responses to Huawei security risks—and to risks posed by really any hardware and software in the U.S. digital supply chain—don't have to be this way. The U.S. government has the opportunity to develop objective, consensus-based trust criteria for hardware and software systems. It could then use those criteria to make and explain evidence-based analyses on the risks posed by technology like Huawei's 5G equipment—as well as developing strategies about what to do about it.

"This is a process that would help the U.S. build a robust, long-term strategy for making digital supply chain security decisions. And in Huawei's case, where there are clear national security risks surrounding backdoors (vulnerabilities inserted at a government's behest), bugdoors (accidental flaws which the government says to leave in place) and regular vulnerabilities (just plain accidental), this shouldn't be difficult. Quite the contrary, in fact." // LAWFARE

ALTERNATIVE OPTION THREE

International Cyber Peace Treaties and Mutual Trust Agreements. History has shown that when countries are damaging themselves more from war than the potential spoils or ideology gains, they seek, it is wise to sign a peace treaty. If the countries are building weapons that are expensive and could destroy the world many times over, it makes more sense to sign a non-proliferation treaty. In fact, countries from around the world have signed many different kinds of treaties in order to help the world advance and not be stuck in the chaos of conflict.

The U.S. could be the world leader in developing a new kind of peace treaty or mutual trust agreement the world has not yet seen – a cyber conflict treaty. Global norms could be negotiated and agreed to by multiple countries who then sign an agreement to abide by the terms. There are groups already working on creating a common understanding of information security, such as the United Nations Group of Governmental Experts (UNGGE), and the Global Initiative on Data Security announced by the Chinese government on Sept 8, 2020.

Note that China has at least taken the first step to start a discussion on a global initiative with data security. Think of the progress that could be made if the U.S. was willing to partner with them in this effort instead of isolate from this possibility.

One critical area of progress we could get from agreement to international norms, terms and common understandings could be a greater ability to attribute the source of attacks and the means by which they were carried out. Instead of each country fighting the cyber battle independently, we could be stronger when united. Which is the way we have successfully approached the threat of nuclear war by the way.

This agreement between two or more countries would be put in place to protect the signers from cyber aggression from the other signers with the intent to gain some kind of market or political advantage. As with other kinds of treaties/agreements, removing the potential conflict allows the signers to invest their energy on more productive tasks than defending themselves.

It is time for the U.S. to build an international coalition to construct a framework for a cyber peace treaty and deescalate the growing efforts to harm each other through the digital attacks. Much like past peace/trust treaties, countries that choose to be outside the treaty will then be shunned from the international community and will face a collective response from the countries that have chosen peace and how have available security resources to focus tightly on the outlier countries.

ALTERNATIVE OPTION FOUR

International Digital Security Oversight Coalition. In the past 100 years, countries have come together to create international bodies to provide safety, security and conflict de-escalation. The United Nations was founded after two world wars in order to help countries resolve differences without the need to choose sides and create massive worldwide conflicts. An international body that has the responsibility to assure that technology does not get weaponized and sold to unsuspecting buyers would make sense for the future. More than that, a coalition that can help oversee the safety of digital devices and systems worldwide would help us avoid what could be disastrous consequences.

This could become possible through utilizing a crawl, walk, run approach. The first task of the organization would be to define what would be considered wrongdoing. The second task would be to suggest measures for improvement in tracking and testing. Later, they could integrate consequences for repeat offenders.

This may sound like an idea that is just too hard to execute on, yet we have really good examples of how we have solved safety and security problems in this way already. Underwriters Laboratories (UL) was founded in 1894 in order to provide safety testing for any product that used electricity. They came about to solve the problem of manufacturers who would be less than responsible with product designs to keep consumers from being electrocuted by their products. Today UL serves customers in more than 104 countries.

We need neutral countries to help sponsor this kind international coalition and not depend on the U.S. to do the heavy lift, however, the U.S. can be very helpful with using our economic presence to support the coalition. Much like the UL, this coalition can help develop rules and practices for security and data privacy that must be imbedded into products and applications. If any company is found to violate the boundaries set by this group, the coalition would have the backing to levy financial penalties and advertise worldwide so people (customers) would know to avoid doing business with the offending provider. This would make it unfeasible and unwise for a company to sell products that could be used in a cyber abusive manner.

CONCLUSION

The Trump administration started the U.S. down a path towards blacklisting companies they believed exhibited a current or possible risk. The administration also put orders in place that restricted who U.S. technology providers could sell to. This should not be compared to blocking business access to a country like Iran in order to put political pressure on its leaders to change behaviors. In that case there is a justifiable reason to embargo U.S. companies from selling into the offending country.

The restrictions on technology organizations in this case were actions against companies that do business internationally and are domiciled at least partially in a country of concern from a cybersecurity standpoint. Although the motivations might make sense on the surface, the outcome is not positive enough to continue this policy direction.

"The notion of a broad ban on TikTok is a bad idea. As mentioned, there is no clear government-presented evidence that TikTok poses a national security threat to the average US consumer (again, federal employees are a different case). Some in Washington, this administration included (referring to the Trump administration), may love the idea of expelling all technology from the country that has any connection to China.

"But that approach simplifies complex supply chain security decisions—about data localization, about encryption, about trusting an app's software updates—and boils it all down to a single country-of-origin data point with seemingly little appreciation for the repercussions. It also raises urgent questions about unilateral decisions to prohibit Americans from using foreign software." // *NEW ATLANTICIST*

We now have a new administration taking over the American Executive Branch. This gives us a wonderful opportunity to be world leaders in strengthening cybersecurity defenses for the U.S. and other countries as well. The world needs transparent rules that all companies can comply with in order to increase innovation and protect citizens against cybercrime.

It is our sincere desire that this paper helps frame the problems and provide strong alternatives. Our political leaders need to be collaborative partners with our business leaders and find a path forward that will address the very real problems cyberwarfare and cybercrime foster while not shutting the U.S. economy off from the rest of the world.

ABOUT THE AUTHOR

Scott Klososky is the founder of Future Point of View LLC., a digital strategy firm. He has had a long career in building technology startups and advising clients on digital strategy plans. He led projects done in Russia, China, and many other countries around the world. He is well known on the speakers circuit for accurately predicting the future of the Digital Transformation.

FPOV
FUTURE POINT OF VIEW