Cyber Border Security: Defining and Defending the National Cyber Border

Purpose

What this presentation is…

Explores the interpretation, adaptation, and application of traditional border domain concepts in order to define, defend, and enforce a national cyber border.

Discusses one approach to a complex issue

What this presentation isn‘t…

A complete treatment of a complex issue.

Leaves much of the “How” of enforcing and defending the cyber border to future research and debate.

The Need

Border security is a critical component of homeland and national security.

The border is where foreign threats become domestic realities.

Border and Cyber threats from criminals, terrorists, and hostile nation states present dangers to homeland and national security.

Border protections- extensive (CBP, BP, USCG, DOD) and codified in laws
Cyber protections-largely voluntary and spread across public and private sectors.

Cyber and Border threat convergence
Cyber allows circumvention of traditional border domain security measures (i.e., importation of contraband, export/exfiltration of sensitive/protected information, cross border movement of funds), and also presents unique attack/threat vectors.

Cyber threats perhaps more dangerous due to their asymmetrical nature and interdependency issues.

How

By evolving our concept of borders to include the cyber domain.

Thus allowing the development of refined policies and protective strategies to defend and enforce the nation’s cyber border.

- Where wires cross the border is insufficient and incomplete.

Key concept- Functional Equivalents of the Border (FEBs)

1) A “nexus” to the border, a border crossing, or to something which has crossed the border
2) A reasonable certainty that there has been no material change since the nexus with the border
3) The search and/or inspection occurs at the first practical detention point after the border crossing

By using existing border authorities and protections

- Nations have an absolute right to control who and what crosses their borders.
- Border inspection- well established exception to 4th amendment – allowing inspections, searches, and seizures at the border or their FEB.
- Searches/inspection of People, Conveyances, and Cargo and for **Merchandise, Documents, and Contraband**.
- Should cyber delivered imported/exported merchandise enjoy greater privacy or be exempt from border controls compared to its physical domain equivalent? Why?

Merchandise

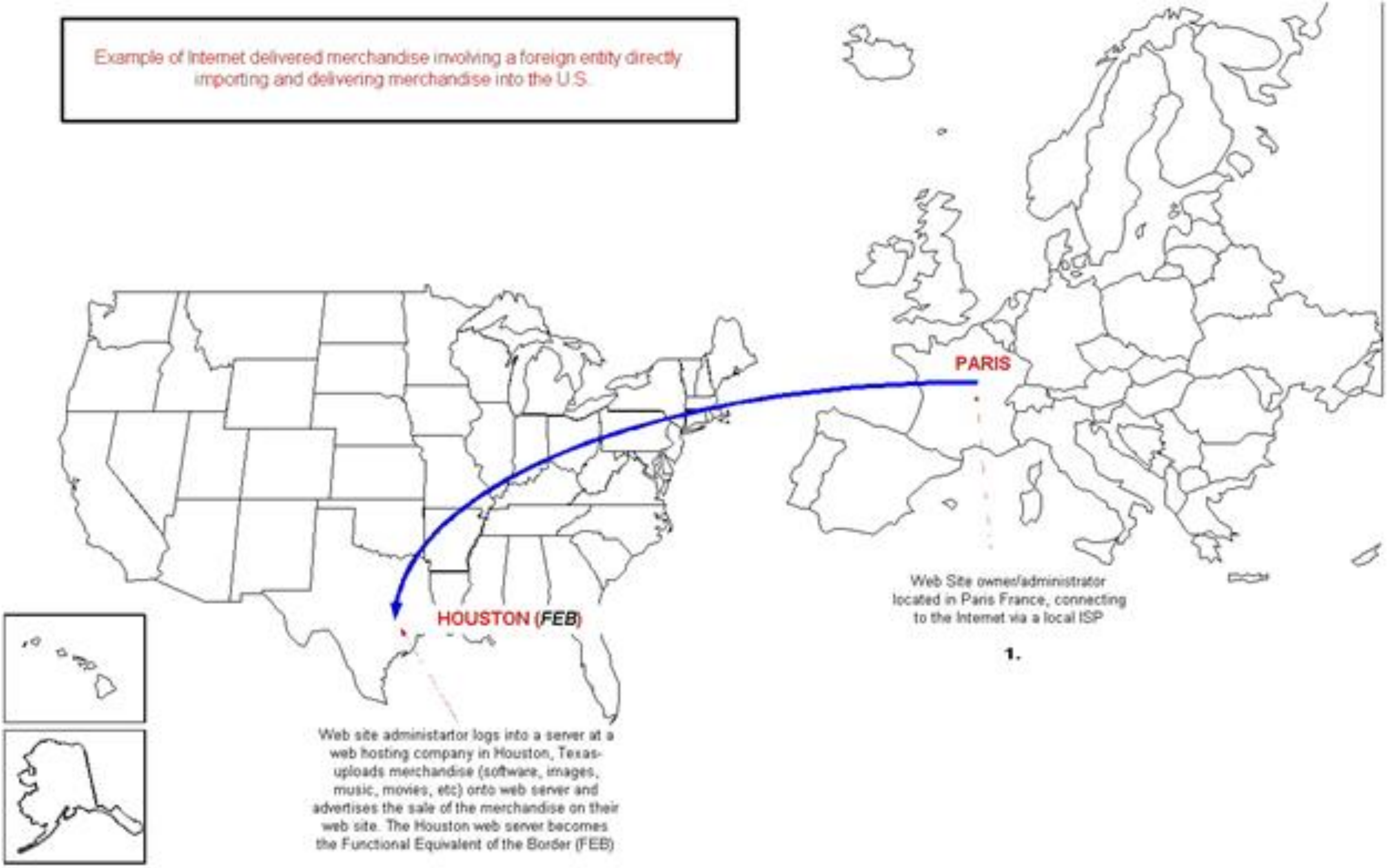
Def. “Goods, wares, and chattels of every description”. … 19 CFR 146.1

Contraband- Imports or exports contrary to law

Privacy Concerns

- Lower expectation of privacy at the border
- Private or privileged communications are already have protections from inspection under current border search authorities.
- Documents relating to merchandise or contraband being imported/exported are subject to inspection.

Example of Internet delivered merchandise involving a foreign entity directly importing and delivering merchandise into the U.S.



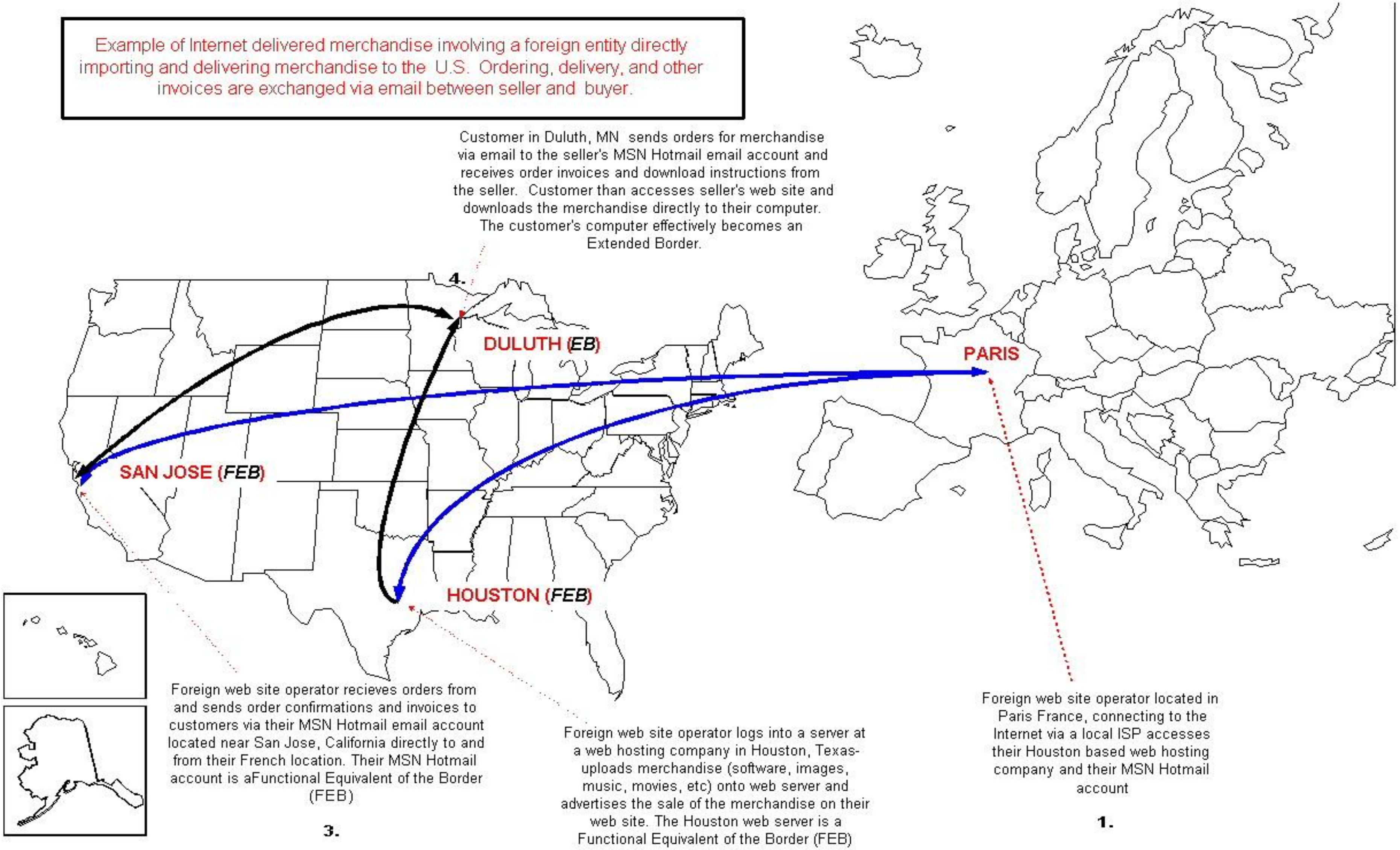
Web Site owner/administrator located in Paris France, connecting to the Internet via a local ISP

1.

Web site administartor logs into a server at a web hosting company in Houston, Texas- uploads merchandise (software, images, music, movies, etc) onto web server and advertises the sale of the merchandise on their web site. The Houston web server becomes the Functional Equivalent of the Border (FEB)

2.

Example of Internet delivered merchandise involving a foreign entity directly importing and delivering merchandise to the U.S. Ordering, delivery, and other invoices are exchanged via email between seller and buyer.



Foreign web site operator located in Paris France, connecting to the Internet via a local ISP accesses their Houston based web hosting company and their MSN Hotmail account

1.

Foreign web site operator logs into a server at a web hosting company in Houston, Texas- uploads merchandise (software, images, music, movies, etc) onto web server and advertises the sale of the merchandise on their web site. The Houston web server is a Functional Equivalent of the Border (FEB)

2.

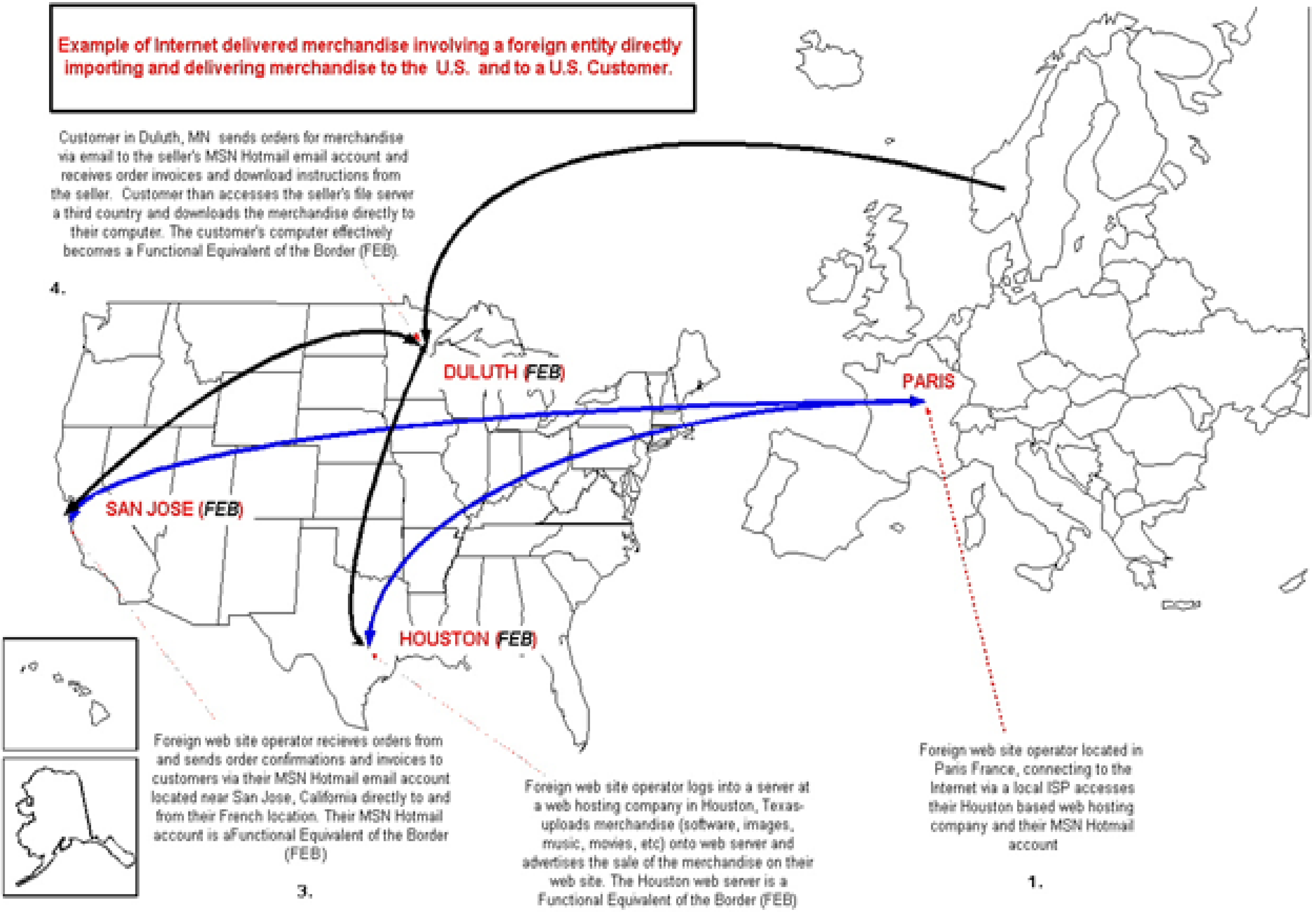
Foreign web site operator recieves orders from and sends order confirmations and invoices to customers via their MSN Hotmail email account located near San Jose, California directly to and from their French location. Their MSN Hotmail account is aFunctional Equivalent of the Border (FEB)

3.

4.

Customer in Duluth, MN sends orders for merchandise via email to the seller's MSN Hotmail email account and receives order invoices and download instructions from the seller. Customer than accesses seller's web site and downloads the merchandise directly to their computer. The customer's computer effectively becomes an Extended Border.

Example of Internet delivered merchandise involving a foreign entity directly importing and delivering merchandise to the U.S. and to a U.S. Customer.



Customer in Duluth, MN sends orders for merchandise via email to the seller's MSN Hotmail email account and receives order invoices and download instructions from the seller. Customer than accesses the seller's file server a third country and downloads the merchandise directly to their computer. The customer's computer effectively becomes a Functional Equivalent of the Border (FEB).

4.

Foreign web site operator recieves orders from and sends order confirmations and invoices to customers via their MSN Hotmail email account located near San Jose, California directly to and from their French location. Their MSN Hotmail account is aFunctional Equivalent of the Border (FEB)

3.

Foreign web site operator logs into a server at a web hosting company in Houston, Texas-uploads merchandise (software, images, music, movies, etc) onto web server and advertises the sale of the merchandise on their web site. The Houston web server is a Functional Equivalent of the Border (FEB)

2.

Foreign web site operator located in Paris France, connecting to the Internet via a local ISP accesses their Houston based web hosting company and their MSN Hotmail account

1.

Conclusion

Just one approach based on the interpretation and adaptation of existing laws.

No solution is 100 percent effective- no matter what the domain.

As cyber threats evolve and increase, doing nothing is not an option.

The “cannon shot rule” (Cornelis van Bijnkershoek, Hugo Grotius**)**

One solution is the development of policies and strategies based on the adaptation of existing authorities which are anchored in centuries of legal precedence.

Questions?

posborn@gmail.com