The Internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify?

Joel P. Trachtman
The Fletcher School of Law and Diplomacy

Outline of Presentation

- **Introduce and Define Terms and Regulatory Concerns**
- Describe Cybersecurity Risks of IoT
- Describe Growing National Standards
- Analyze Legal Issues Raised by Defensive Strategies
  - Prohibitions
  - Security Exceptions
- Posit a Cooperative Strategy to Minimize Disruption of Trade and Investment, Without Compromising Cybersecurity
- Questions/comments welcome along the way . . . .

What is the IoT?

Consumer

- Toys
- Smart speakers
- Appliances
- Autos
- Medical devices
- Etc.

Industrial/Infrastructural/Transport

- Industrial controllers
  - Nuclear—Stuxnet
  - Factories
- Communications and energy grids
- Aircraft
- Trains
- Etc.

ISO Definition:

- IoT is defined as an infrastructure of interconnected physical entities, systems and information resources together with the intelligent services which can process and react [to] information of both the physical world and the virtual world and can influence activities in the physical world.
- Note connected nature; constant risk of hacking

National Motivations: Political Economy of IoT Defense

- Ordinary regulatory concerns
- Security concerns
- Competitive concerns
- Geoeconomic concerns
- IoT as threat to security→security as threat to trade→isolation as threat to technological development/security

Outline of Presentation

- Introduce and Define Terms and Regulatory Concerns
- **Describe Cybersecurity Risks of IoT**
- Describe Growing National Standards
- Analyze Legal Issues Raised by Defensive Strategies
  - Prohibitions
  - Security Exceptions
- Posit a Cooperative Strategy to Minimize Disruption of Trade and Investment, Without Compromising Cybersecurity

Risks

- Attack on individual or other non-governmental privacy,
- Disinformation or other less serious attack on system integrity,
- Less serious physical attack on individuals or property,
- Espionage against governments,
- Attack on critical infrastructure, or
- More serious physical attack on individuals or property

High risk IoT and Low risk Iot

- High risk = unacceptable/catastrophic consequences = security risk
- Low risk IoT can be used to attack high risk IoT; Botnet
- Analytical tool
- Legal significance:
  - Ordinary regulation versus high security regulation
  - International law significance: management of trade effects of ordinary regulation versus management of security risks

Huawei and the 5G Analogy/Relationship

- Risk of foreign control of national telecommunications system
  - Privacy
  - Security
  - Disabling
  - Weaponizing
- 5G as the “backbone” of IoT
- U.S. concerns and Australia, UK, etc.

UK Approach to Huawei 5G

- Huawei Cyber Security Evaluation Centre (HCSEC) established “under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK’s critical national infrastructure.”
- Oversight Board: (i) assesses independence and competence, (ii) assesses risk from products
- Problems of “consistent build” to evaluated binary; secure chain of custody; evaluating updates
- 4/24/19: PM Theresa May decides to allow Huawei to supply “non-core” portions of 5G network

Outline of Presentation

- Introduce and Define Terms and Regulatory Concerns
- Describe Cybersecurity Risks of IoT
- **Describe Growing National Standards**
- Analyze Legal Issues Raised by Defensive Strategies
  - Prohibitions
  - Security Exceptions
- Posit a Cooperative Strategy to Minimize Disruption of Trade and Investment, Without Compromising Cybersecurity

Nascent National Standards: Consumer Products

- IOS “reference architecture”—descriptive not normative:
  - Robustness, reliability, resistance
  - Confidentiality, data integrity, safety, protection of personally identifiable information
- UL (Underwriters Laboratories) 2900
- Cellular Technology Industry Association
- UK Department of Culture, Media, and Sport Guidance
- GDPR
- California statute
- Tendency to move to highest common denominator: California or Brussels Effect

Nascent National Standards: High Risk IoT

- NIST 2/1/2019 Discussion Draft re Core IoT Cybersecurity Capabilities Baseline
- US NIST Goals for Industrial Control—Apply to high risk IoT
  - Resist electronic and physical access to network and components
  - Prevent unauthorized modification of data
  - Detect and report security events
  - Maintain robustness of network and components
- NIST Framework 1.1:
  - Identification of risk
  - Protection from harm
  - Detection and response to intrusion
  - Recovery
- European Union Agency for Network and Information Security (ENISA)—baseline security recommendations for critical infrastructure

Outline of Presentation

- Introduce and Define Terms and Regulatory Concerns
- Describe Cybersecurity Risks of IoT
- Describe Growing National Standards
- **Analyze Legal Issues Raised by Defensive Strategies**
  - **Prohibitions**
  - **Security Exceptions**
- Posit a Cooperative Strategy to Minimize Disruption of Trade and Investment, Without Compromising Cybersecurity

Defensive Strategies Available to States

- Ban all IoT (including domestic)
- Establish product standards for public procurement
- Establish product standards for private procurement
- Establish producer standards—trusted manufacturers
- Restrict foreign investment in IoT production
- Combinations

Trade and Investment Law Issues

- Discrimination: GATT, TBT, and GATS national treatment and MFN
  - Product standards
  - Producer qualifications
- TBT adds proportionality, international standards
- WTO Government Procurement Agreement (GPA)
- Investment market access restriction prohibitions under bilateral investment treaties (BITS)
- General exceptions
- Security exceptions

National Treatment and MFN

- GATT, TBT, GATS
- Like products defined by competition
- Less favourable treatment defined by effects on competition
- Little room for regulatory purpose in GATT: if consumers fail to distinguish, could violate NT or MFN
- Because no general exceptions in TBT, understood differently: not less favourable if “stems exclusively from a legitimate regulatory distinction”
- Questionable space to regulate/surveil production process
- Distinctions based on location (or identity) of producer, including home country regulation or statecraft, would ordinarily violate NT or MFN

Additional TBT Requirements

- Proportionality
- Utilize international standards as basis unless ineffective—do not contradict
  - No international standards yet

Argentina—Financial Services (AB 2016)

- AB refused to make a finding on whether services of companies from tax non-cooperating countries (Panama) are “like” services of tax cooperating countries, or Argentinean companies
- Analogous to question of conditioning market access to home country IoT regulation

General Exceptions: GATT Art. XX

- Apply only within GATT
- Art. XX(b): necessary to protect human life or health
- Art. XX(d): necessary to enforce laws, including to avoid deceptive practices
- Subject to chapeau requirements of reasonableness, non-arbitrariness—is differential treatment of home countries reasonable?
- Necessity as “least trade restrictive alternative”; balancing
- Similar exceptions in GATS, but not in TBT

Security Exceptions: GATT Art. XXI (none in TBT)

- “which it considers necessary for the protection of its essential security interests
  - relating to traffic in arms, ammunition, and implements of war
  - In time of war or other emergency in international relations
- ”Traditional” U.S. position that these are self-judging, non-justiciable (inconsistent with U.S. travaux preparatoires: Mona Pinchis-Paulsen)
- Recently “adopted” panel decision in Russia—Trade in Transit finds
  - Justiciable
  - Not self-judging
  - Parameter of “emergency in international relations” objectively determinable
  - “essential security interests” relate to quintessential functions of state—invocation must be specific

Summarizing on Exceptions

- For low risk IoT, either no violation of WTO law, or general exception if comply with Art. XX(d) or XX(b)—necessity, no arbitrary or unjustifiable discrimination
  - Question whether discrimination against China would be arbitrary or unjustifiable
- For high risk IoT, security exception under Art. XXI(b)(iii) emergency, or XXI(b)(ii) implements of war; may also be excepted under Art. XX(b)
- TBT lacks general exceptions, security exceptions
- GATS and GPA track GATT, except
  - GATS Art. XIV adds to general exceptions “necessary to protect public order”
  - GPA Art. III security exception: procurement of war materials or indispensable for national security

	Possible GATT violations	GATT security exception	GATT general exception	Possible TBT violations	No TBT security or general exception
Low Risk IoT	Little need to violate national treatment or MFN	XXI probably unavailable	XX(b),(d) probably available	2.1 (national treatment or MFN) 2.2 (proportionality) 2.4 (use international standards)	
High Risk IoT	III:4 I (MFN)	XXI possibly available	XX(b) possibly available	2.1 2.2 2.4	

Outline of Presentation

- Introduce and Define Terms and Regulatory Concerns
- Describe Cybersecurity Risks of IoT
- Describe Growing National Standards
- Analyze Legal Issues Raised by Defensive Strategies
  - Prohibitions
  - Security Exceptions
- **Posit a Cooperative Strategy to Minimize Disruption of Trade and Investment, Without Compromising Cybersecurity**

High Risk IoT

- Need to distinguish among suppliers based on security
- Availability of security exception unclear
- Core security procurement likely to be subject to security exception
- Trade will be impeded without cooperative solution
- HCSEC as model for verification—difficulties
- IAEA NPT inspection model
- Hacking prevention critical
- Combination of trust and verification—sliding scale based on nationality of control?

Low Risk IoT

- Security exception likely unavailable
- General exceptions available, if measure necessary, reasonable, non-arbitrary, but problem of TBT
- International standards solve part of the problem of TBT: deemed proportionate (not deemed non-discriminatory)
- Food analogy: systems recognition; equivalence; on-site verification
  - Argentina: Financial Services
- Combination of trust and verification—sliding scale based on nationality of control?

Trust and Verification Matrix

	Certified Supplier	Non-Certified Supplier
Low Risk IoT	Light verification of security design and anti-hacking	Intermediate verification of security design and anti-hacking
High Risk IoT	Intermediate verification of security design and anti-hacking	Maximum verification of security design and anti-hacking

Conclusions

Incentives to cooperate to maintain trade and investment

Low risk IoT not very different from other products

High risk IoT is distinct

- Catastrophic risk
- Unclear security exception
- Need for sliding scale of trust and verification