
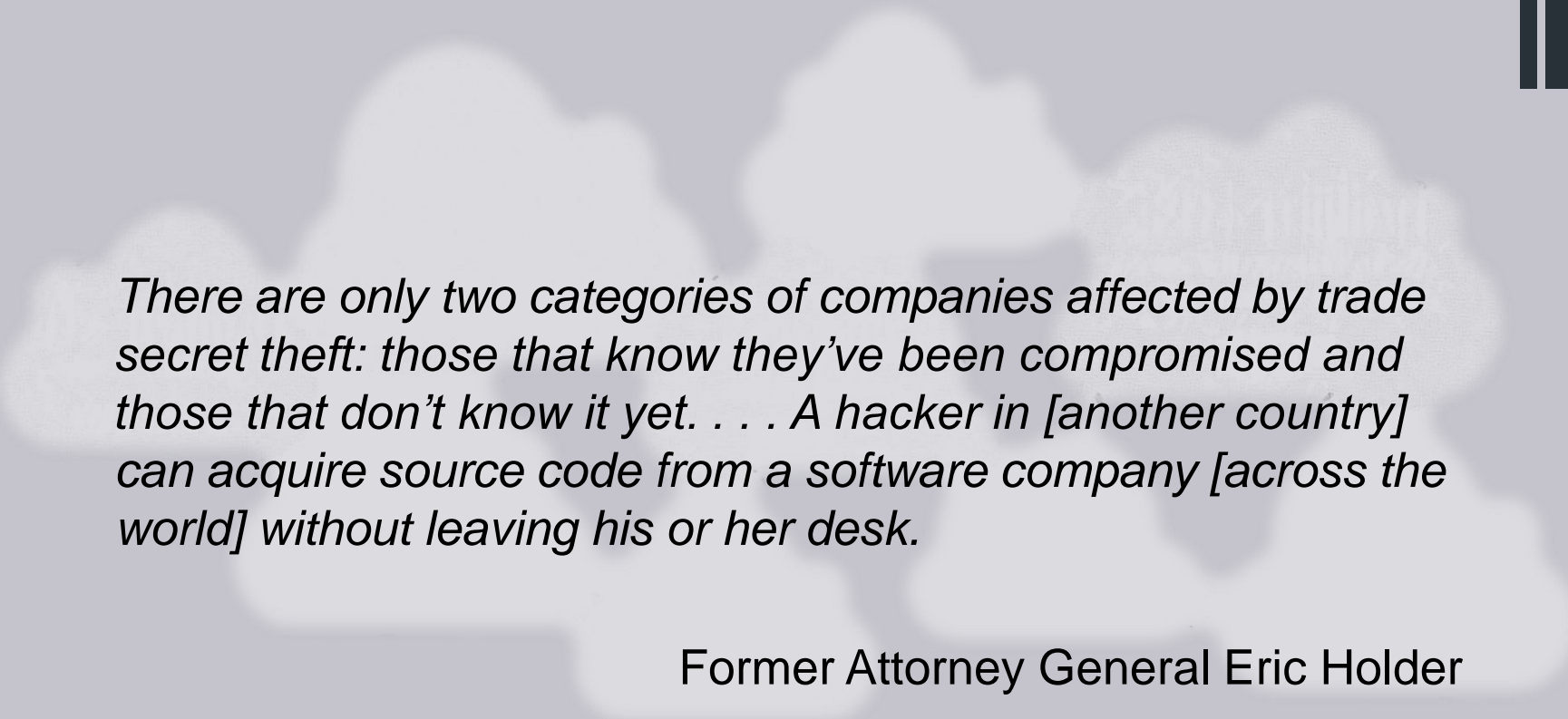




Policing and Litigating Digital Trade Secrets

Ryan Hersh
J.D. Candidate | Class of 2017
University of Connecticut School of Law
55 Elizabeth Street
Hartford, Connecticut 06105



There are only two categories of companies affected by trade secret theft: those that know they've been compromised and those that don't know it yet. . . . A hacker in [another country] can acquire source code from a software company [across the world] without leaving his or her desk.

Former Attorney General Eric Holder



Presentation Overview

- The Backdrop
- The Trade-Secret Plaintiff
- The Cloud-Storage Provider
- The Trade-Secret Defendant
- The International Trade-Secret Misappropriation
- The Future: Some Remaining Issues

The Backdrop: Trade-Secret Law

- Legal Elements

1. Not Generally Known or Readily Ascertainable
2. Commercial, Economic Value
3. Reasonable Measures to Maintain Secrecy



The Backdrop: Increasing Importance

- Benefits Compared with other Intellectual-Property Rights
- Recent Rise in Trade-Secret Litigation
- Media and Scholarly Attention
- Economic and Commercial Value
- Increasing Use of Cloud Storage
- Global Importance
 - TRIPs and TRIPs+, Defend Trade Secrets Act, and EU Directive

The “Traditional” Trade-Secret Plaintiff

- Expensive Protection Measures
 - Physical lock-and-key, vaults, etc.
- High Operating Expenses
 - Required more employees
 - And greater overhead
- Low Recurring Cost
 - Low risk of misappropriation

Impact of the “Cloud”

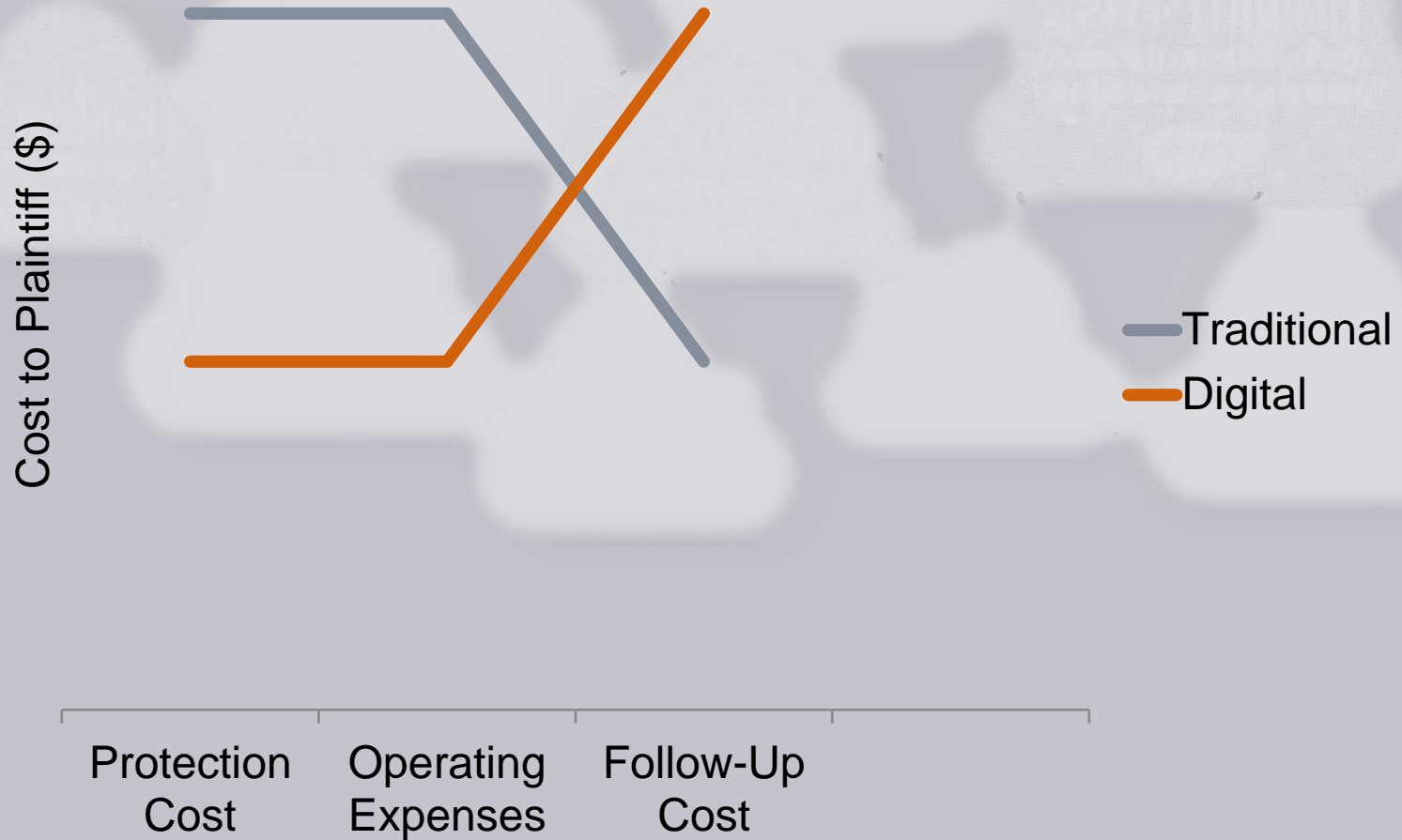
- Recognizable benefits
 - Pay-as-you-go model
 - Deductible as capital expenditure
 - Less equipment, personnel, and maintenance cost
 - Adaptable to personal storage needs
 - Accessible anytime, anywhere



The “Digital” Trade-Secret Plaintiff

- Inexpensive Protection Measures
 - Cloud storage, offsite servers (outsourced)
- Low Operating Expenses
 - Required less employees
 - And lower overhead
- High Recurring Cost
 - Increased risk of misappropriation
 - Costly internal information barriers

Summary: The “Digital” Trade-Secret Plaintiff





The Cloud-Storage Provider

- Three Types of Relationships
 - Traditional Licensing Contracts
 - Designed to offload risk onto trade-secret plaintiff
 - Click-wrap style
 - Liability-exclusion clauses
 - Right-of-access provisions (mostly for advertising)
 - Unilateral cloud-side possibility for termination
 - Lack of equal bargaining power with largest cloud providers (Microsoft, Amazon, Google)



The Cloud-Storage Provider

- Beyond Contract Law to Tort Liability
 - Fiduciary duties to trade-secret plaintiff
 - Duty of confidentiality
 - Duty not to appropriate
 - Negligence claims (high burden on trade-secret plaintiff)
 - Trespass to chattel, conversion
- Natural market forces
 - Competitive incentive to perform well



The “Traditional” Trade-Secret Defendant

- Difficult to misappropriate
- Mostly domestic misappropriation
- Departing employees remained local



Impact of the Cloud

- Easier to access, but also easier to misappropriate (double-edged sword)
- Internationally accessible, allowing for international misappropriation



The “Digital” Trade-Secret Defendant

- Less costly to misappropriate
- International instances of misappropriation
- Departing employees no longer remain local

International Trade-Secret Misappropriation

Pre-May 2016 Framework

- United States
 - State-specific laws
 - 47 “UTSA” states
 - MA-specific statute
 - NY and NJ common-law rules
- Europe
 - Country-specific laws
 - Strict—e.g., Germany
 - Relaxed—e.g., Estonia, Bulgaria
 - Definitional differences—e.g., Sweden

Post-May 2016 Framework

- United States
 - Defend Trade Secrets Act
- Europe
 - EU Directive

DTSA and EU Directive: A Closer Look

DTSA

- Creates federal cause of action
- Harmonizes (UTSA) definition across states
- Permits *ex parte* seizure in “extraordinary circumstances”
 - How does this apply to trade secrets stored in the cloud?
- Rejects inevitable disclosure doctrine

EU Trade-Secrets Directive

- Creates minimum standards for trade-secret protection across EU-member states
- Harmonizes definition across EU-member states
- Permits disclosure in accordance with specific state rules
- Reinforces importance of employee mobility

Bringing it all Together

- DTSA and EU Directive should help—but more is needed
- Action is needed at two levels:
 1. Practical—trade-secret plaintiff
 2. Normative—convergence across jurisdictions

Level 1: Trade-Secret Plaintiff and Best Practices

1. Prior to choosing the cloud-storage provider

1. Ensure data networks are secure
2. Understand cloud-storage provider's intentions with trade secrets
3. Clear, enforceable contracts
 1. Choice-of-law and forum-selection clauses
 2. No commingling with other customers' trade secrets
4. Understand cloud-storage provider's jurisdiction

Level 1: Trade-Secret Plaintiff and Best Practices

2. After choosing the cloud-storage provider

1. Internal practices

1. Restrict employee access to cloud-stored trade secrets
1. Limit downloading from cloud
1. Employ knowledgeable IT team
1. Be aware of and respond to required state- or country-specific practices

1. Monitor chosen cloud-storage provider

1. Switch providers if current provider is slow to progress
2. Diversify trade-secret portfolio across providers

Level 2: Convergence Across Jurisdictions

- TRIPs should directly define and address trade secrets
- Need for uniformity across WTO member-state jurisdictions
- Normative Issues
 - Jurisdiction-Related Issues
 - Tort—location of misappropriation
 - But what is the location?
 - Physical location of cloud-storage provider's servers
 - Physical location where trade-secret defendant misappropriated
 - Cloud-Storage Provider Issues
 - Duties and obligations outside contract law
 - But what are those duties?
 - Strict—no commingling trade secrets, no advertising, no self-dealing, etc.
 - Relaxed—only where actions place trade-secret defendant at competitive advantage



Questions and Comments

Thank You