cloud security alliance

CSA

privity

Governance, Risk Management, Compliance, & Audit

An Overview of Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing

July 23, 2009

Agenda

- About the Presenter
- About the Cloud Security Alliance
- Guidance 1.0
- Getting Involved
- Call to Action

About the Presenter

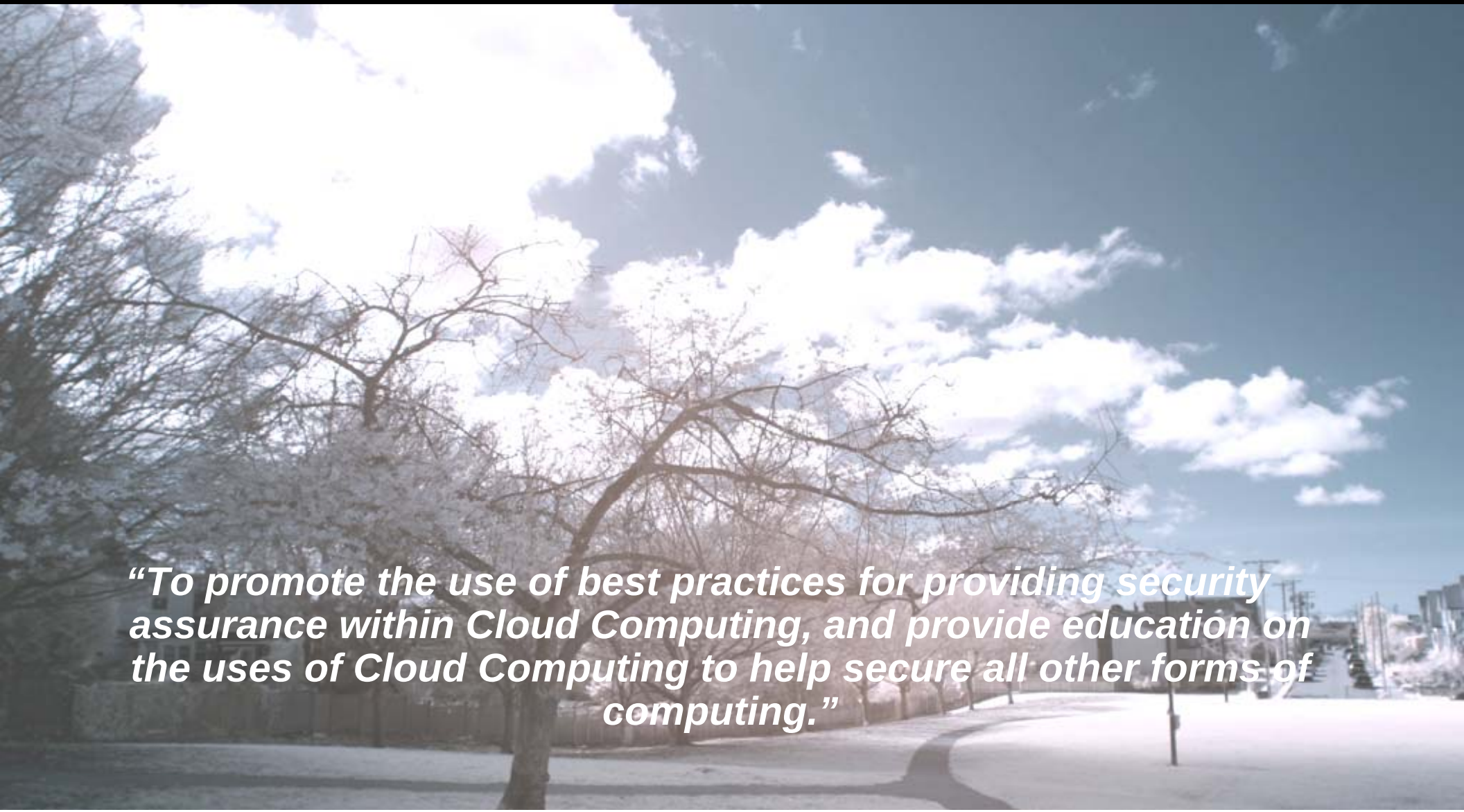
Shawn R. Chaput

Chief Architect & Executive Consultant, Privity Systems Inc.

- **ABCP** (Certified Associate Business Continuity Professional) [DRII] .
- **CFE** (Certified Fraud Examiner) [ACFE].
- **CIA** (Certified Internal Auditor) [IIA].
- **CIPP/C** (Certified Information Privacy Professional / Canada [IAPP].
- **CGEIT** (Certified in Governance of Enterprise IT) [ISACA].
- **CISA** (Certified Information Systems Auditor) [ISACA].
- **CISM** (Certified Information Security Manager) [ISACA].
- **CISSP** (Certified Information Systems Security Professional) [ISC^2].
- **ISSAP** (Certified Information System Security Architecture Professional) [ISC^2].
- **ISSMP** (Certified Information Systems Security Management Professional) [ISC^2].
- **PMP** (Project Management Professional) [PMI].

- **Founding Member of Cloud Security Alliance**
- **Principle Author of Audit & Compliance Section of Guidance 1.0**

About the Cloud Security Alliance



cloud security alliance

privity

cloud security alliance

privity

Governing the Cloud

Download at:
www.cloudsecurityalliance.org/guidance

Overview of Guidance

1. Architecture & Framework

Governing in the Cloud

2. Governance & Risk Management
3. Legal
4. Electronic Discovery
5. Compliance & Audit
6. Information Lifecycle Management
7. Portability & Interoperability

Operating in the Cloud

8. Traditional, BCM, DR
9. Data Center Operations
10. Incident Response
11. Application Security
12. Encryption & Key Mgt
13. Identity & Access Mgt
14. Storage
15. Virtualization

Assumptions & Objectives

- **Cloud Adopters vs. Security Practitioners**
- **Broad “Security Program” Perspective**
- **Strategic and Tactical Approach**
- **Cloud Models Difference Driven**

Governance & ERM

Cost Shifting

Third Party Transparency

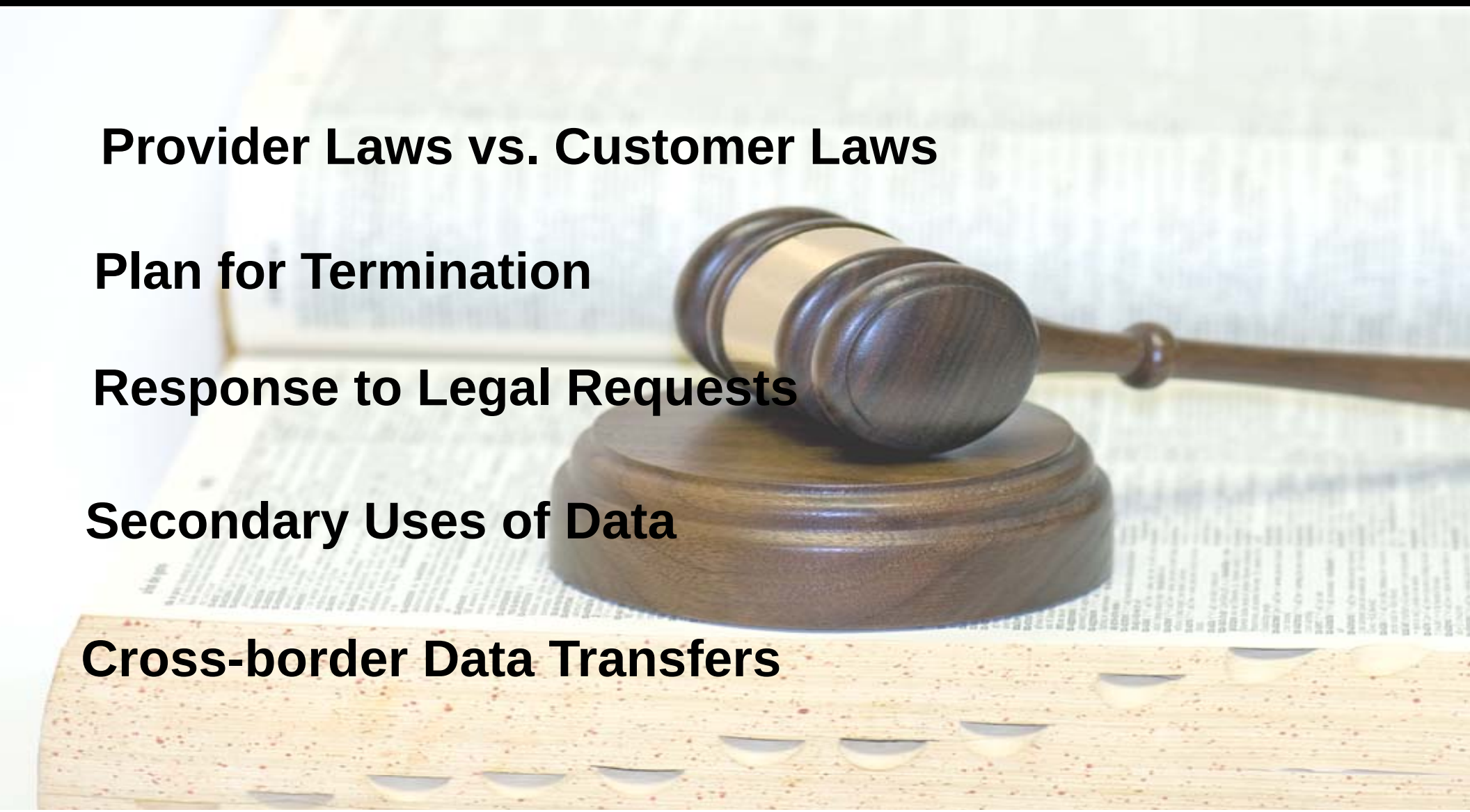
Financial Viability

KPI Alignment

PII Concerns

Risk Assessments

Legal



Provider Laws vs. Customer Laws

Plan for Termination

Response to Legal Requests

Secondary Uses of Data

Cross-border Data Transfers

Electronic Discovery

Impact on Records Information Management

Roles and Responsibilities

Control Data

Preserve Data

Compliance & Audit

- **Classify Data and Systems**
- **Data Locations, Copies**
- **Minimum Periodic Audits**
- **Understand Scopes**
- **Right to Audit**

Information Lifecycle Mgt

Segregation of Data from Protective Controls

Segregation of Duties

Privacy Restrictions

Data Retention Assurance

Data Destruction

Recovering True Cost of a Breach

Portability & Interoperability

Layers of Abstraction

Regular Data Extractions and Backups (SaaS)

Applications Abstracted from the Image (IaaS).

“Loose Coupling” (PaaS)

Migration to Competitor Capability

Advocate Open Standards.

Summary

- Cloud Computing is real and transformational
- Cloud Computing can and will be secured
- Broad governance approach needed
- Tactical fixes needed
- Combination of updating existing best practices and creating completely new best practices
- Common sense not optional

Version 2.0

- Group 1: Architecture & Framework
- Group 2: Governance, Risk Management, Compliance, Audit, Physical, BCM, DR
- Group 3: Legal & eDiscovery
- Group 4: Portability & Interoperability & Application Security
- Group 5: Identity & Access Management, Encryption & Key Management
- Group 6: Data Center Operations and Incident Response
- Group 7: Information Lifecycle Management & Storage
- Group 8 Virtualization & Technology Compartmentalization

Call to Action

Join Us

LinkedIn Discussion & Announcements

Version 2.0 of Guidance Development Underway

Other research initiatives and events

Getting Involved

- **Individual Membership (free)**
  - **Subject Matter Experts for Research**
  - **Interested in Learning**
  - **Admin & Org Help**
- **Corporate Sponsorship**
  - **Help Fund Outreach**
- **Affiliated Organizations**
  - **Joint Projects in the Community Interest**
- **Contact Information on Website**

Contact

schaput@privityinc.com / (778) 227-7303

- **www.cloudsecurityalliance.org**
- **info@cloudsecurityalliance.org**
- **Twitter: @cloudsa, #csaguide**
- **LinkedIn: www.linkedin.com/groups?gid=1864210**

Questions?