2017 UT SYSTEM
LEGAL CONFERENCE

presented by the Office of General Counsel

THE UNIVERSITY *of* TEXAS SYSTEM | FOURTEEN INSTITUTIONS, UNLIMITED POSSIBILITIES.

Session 5b

Privacy, Data Security and Legal Considerations in Software as a Service and Cloud Computing Services for Educational Institutions

Presented by:

Cristina Blanton
Associate Systemwide Compliance and
Privacy Officer,
The University of Texas System

Erin Fonte
Member,
Dykema Gossett PLLC

September 28, 2017 2:45-3:45 pm

Privacy, Data Security and Legal Considerations in Software as a Service and Cloud Computing Services for Educational Institutions

Cristina Blanton, U.T. System
Erin Fonte, Dykema Gossett PLLC

University of Texas System Legal Conference
September 28 – 29, 2017

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

Disclaimers

- The opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the opinions of Dykema or The University of Texas System.

- This presentation is an educational tool that is general in nature and for purposes of illustration only. The materials in this presentation are not exhaustive, do not constitute legal advice and should not be considered a substitute for consulting with legal counsel. Neither Dykema nor The University of Texas System has an obligation to update the information contained in this presentation.

Outline of Presentation

- What are software-as-a-service ("SaaS") and cloud services and how do they work?
- Differences between private, public, and hybrid clouds, and associated risks
- Business benefits of utilizing SaaS/cloud services
- Business/Legal risks to consider
- Unique elements of SaaS/cloud services for educational institutions (FERPA and more)
- Emerging SaaS/cloud services issues regarding connected devices and Internet of Things ("IoT")

What are software-as-a-service ("SaaS") and cloud services and how do they work (cont'd)?

- **What is SaaS/cloud computing?**

  - U.S. Department of Commerce, National Institute of Standards and Technology: "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

  - A form of distributed computing capability spread over a network of connected computers or servers

  - <u>Examples</u>: Hotmail, Gmail, Shutterfly, Facebook, Salesforce.com (and many, many others)

What are software-as-a-service (“SaaS”) and cloud services and how do they work (cont’d)?

- **What is SaaS/cloud computing (cont’d)?**
  - U.S. Department of Commerce, National Institute of Standards and Technology – 5 characteristics:
    - **On-demand self-service** – consumer has the ability to provision computing capabilities as needed without requiring human interaction with each service provider
    - **Broad network access** – capabilities are available over the network and accessed through standard mechanism that promote use by heterogeneous thin or thick clients
    - **Resource pooling** – service provider’s resources are pooled to serve multiple consumers
    - **Rapid elasticity** – capabilities can be elastically provisioned and released
    - **Measured service** – metering capability used to control and optimize resources

What are software-as-a-service ("SaaS") and cloud services and how do they work (cont'd)?

- **How do SaaS/cloud services work?**
  - Different levels of cloud computing, each with its own unique set of risks
    - 1) Infrastructure-as-a-Service ("IaaS") – provides companies with a basic set of services to run a computer, including servers, networking, storage, and data center space on a pay-per-use basis. A company using IaaS completely outsources the storage and resources that it needs.

What are software-as-a-service ("SaaS") and cloud services and how do they work (cont'd)?

- **How do SaaS/cloud services work (cont'd)?**
  - 2) Platform-as-a-Services ("PaaS") – provides a cloud-based environment with everything required to build and deliver web-based (cloud) applications.
  - 3) Software-as-a-Services ("SaaS") – is the most basic type of cloud computing. SaaS runs on distant computers in the cloud that are owned and operated by others and connect to users' computers via the Internet, usually a web browser. You have the least control over the cloud in a SaaS agreement.

Differences between private, public, and hybrid clouds, and associated risks

- **How do SaaS/cloud services work (cont'd)?**
- Various deployment and access models:
  - 1) <u>Public cloud</u> (e.g., Google)
    - Can be accessed by any user with an Internet connection and access to the cloud service.
    - Users do not need to purchase hardware, software, or supporting infrastructure because it is owned and managed by public cloud providers.

Differences between private, public, and hybrid clouds, and associated risks

- **How do SaaS/cloud services work (cont'd)?**
- Various deployment and access models (cont'd):
  - 2)<u>Private cloud</u>
    - Owned and operated by a single company with access limited to a specific group of approved users.
  - 3) <u>Hybrid cloud</u>
    - Has both a private and public component and combines two or more cloud deployment models.
    - Can be scaled back and forth on the "public" and "private" portions depending on individual company needs.

Business benefits of utilizing SaaS/cloud services

- Reduced IT costs
- Scalability and computing power
- Business continuity/disaster recovery
- Collaboration efficiency
- Access to cutting-edge technologies and services you cannot build in-house
- Flexibility of work practices (telecommuting, virtual meetings)
- Access to automatic updates and upgrades
- Benefits of platforms for emerging technologies (block chain technology, connected device platforms, etc.)

Business/Legal risks to consider related to data privacy and security

- 1) Defining Services, Cost and Compensation
- 2) Data security
- 3) Data ownership and control
- 4) Data locations and segmentation
- 5) Privacy
- 6) Performance Measures and Service Levels
- 7) Business Resumption and Contingency Plans
- 8) Limitations of liability and indemnification
- 9) Term and Termination
- 10) Insurance

Business/Legal risks to consider related to data privacy and security (cont'd)

- **1) Defining Services, Cost and Compensation**
    - Be sure that the vendor contract clearly and accurately describes services
        - With master services agreements, statements of work ("SOW) and order forms, can be more difficult than you think
    - Compensation, fees, base services and add-ons (beware SOW creep)
    - Who pays for legal, audit and examination fees, and also hardware/software
    - Beware exclusivity (overt and hidden) – exp. "future products"

Business/Legal risks to consider related to data privacy and security (cont’d)

- **2) Data security**
  - Specialized security policies and procedures based on type of data (e.g. protected health information/HIPAA, non-public personal information/Gramm-Leach-Bliley, student personal information/FERPA, card payment information/PCI-DSS)
  - Data breach notification responsibilities
  - Consider payment of expenses resulting from breach
    - Credit monitoring
    - Forensic investigations
  - Vendor should bear the costs of a breach
  - Amount covered should be reasonable to potential exposure
  - Carve out data breach incidents from general limitation of liability caps
  - Timely notification from vendor to you in the event of a breach

Business/Legal risks to consider related to data privacy and security (cont'd)

- **3) Data ownership and control**
  - You should own your own data (employee, students, etc.)
    - Also provisions on vendor's use of "anonymized and aggregate" data
  - Decide who owns jointly developed data
  - Procedures for transitioning back data in the event of termination
  - Charges for post-termination transition
  - Do not allow vendor to destroy your data (e.g., for late payment)
  - Software: consider whether to require escrowing of vendor's software to guard against vendor bankruptcy/dissolution, esp. if customer software developed for your institution

Business benefits of utilizing SaaS/cloud services

- **4) Data locations and segmentation**
  - Physical location of the data that is under the control of the vendor (e.g., European Union)
  - European Union implications/ other country implications
  - Discovery of data by law enforcement or private litigants
  - If vendor will not disclose location of data, request a private cloud arrangement and assurances that data will not be stored or processed in certain countries
  - Data segmentation - Assurances that data will not be stored in the same cloud as competitors’ data

Business benefits of utilizing SaaS/cloud services (cont'd)

- **5) Privacy**
  - How will the vendor be permitted to access, use, or data-mine student or employee data
  - Any individual-facing agreement and other agreements must accurately reflect privacy procedures
  - Documented procedures to protect personally identifiable information your institution shares
  - Request vendor to agree to certify to deletion of data such that it cannot be reconstructed
  - FERPA considerations (more on this below)

Business benefits of utilizing SaaS/cloud services (cont'd)

- FERPA Considerations
  - "University official" exception may apply
  - Consider requiring a Security and Confidentiality addendum
  - Remember the data belongs to the Institution
  - Review privacy notices or policies the vendor intends to use with students, if applicable
  - How will the data be used for the service <u>and</u> after
  - What is the Institution's position on de-identified data

Business benefits of utilizing SaaS/cloud services (cont'd)

- **6) Performance Measures and Service Levels**
  - Define expectations and responsibilities of both parties
  - Basis for monitoring ongoing performance and measuring success, and can trigger rewards or penalties
  - Set standards for business continuity and disaster recovery plans, warranties, up-time guarantees, service and support levels, and response times
  - Calculate up-time guarantees numerically
  - Also specifically clearly remedies and/or monetary penalties for failing to meet up-time guarantees and other service levels
    - TIP: Avoid service level credits – make them write a check to you
  - Industry standards for SLA may provide reference points for commoditized services (e.g. payroll, telecom)

Business benefits of utilizing SaaS/cloud services (cont'd)

- **7) Business Resumption and Contingency Plans**
  - Detailed provisions for continuation of vendor's business function (including system breakdown and manmade disaster) – get a copy of vendor's BCP/DR policies and procedures
  - Vendor responsibilities: back-up; data protection; protecting equipment
  - Third party security audits that include review of BCP/DR issues (e.g. SSAE 16 or SOC 1 audit – new SSAE 18 standard combines these two)

Business benefits of utilizing SaaS/cloud services (cont'd)

- **8) Limitations of liability and indemnification**
  - Damages can be both financial and reputational
  - Liability is usually limited to a fixed amount (e.g. hard dollar cap of last 12 months of fees paid to vendor)
  - Insist on following carve-outs from hard dollar caps: data breach costs, third party IP infringement claims against vendor's technology, and breaches of confidentiality (can be unlimited carve outs, or "split-cap" limits, e.g. separate limit for items carved out of general dollar limit cap)
  - Limitation of liability should be calculated based on expected cost of expenses that would be incurred as part of a data security breach incident
  - Indemnification should include data breach incidents, breaches of confidentiality, and third party IP infringement claims against vendor's technology), and indemnification for these areas should be carved out of hard dollar cap on vendor's liability
  - Vendor should represent and warrant that its third-party service providers will meet the same standards the vendor must meet under the agreement (4th party due diligence)

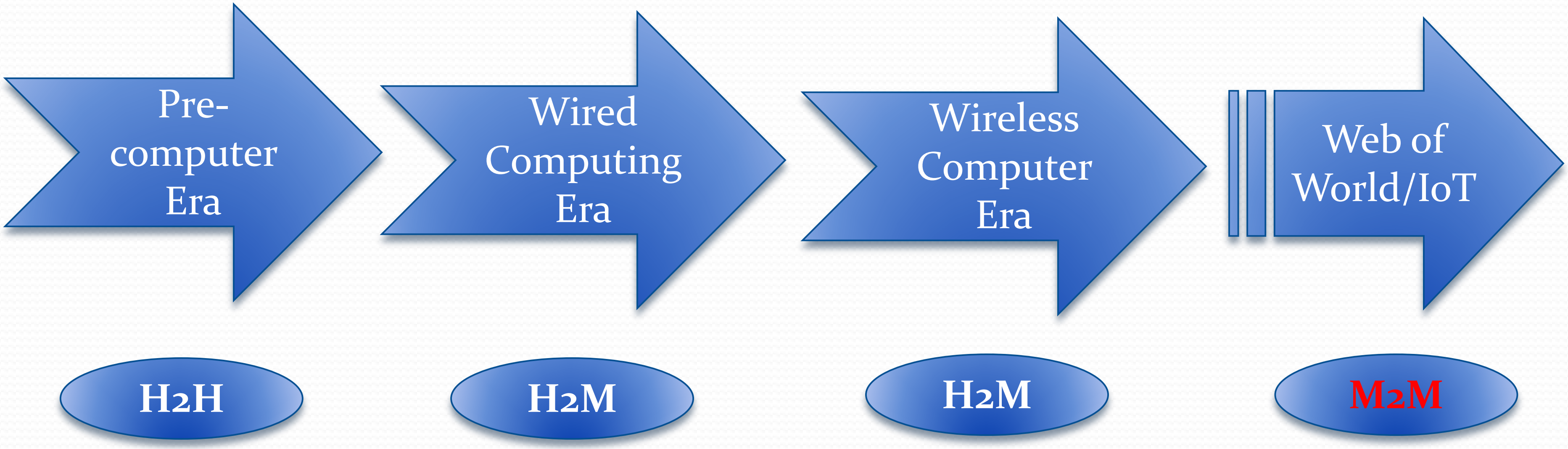
Business benefits of utilizing SaaS/cloud services (cont'd)

- **9) Term and Termination**
  - Careful on the term – have seen initial terms as long as 12 years and auto-renew terms as long as 5 years
  - Unique right to terminate for educational institutions (e.g. violation of FERPA requirements, etc.)
  - Beware termination at will with onerous early termination penalties or liquidated damages (e.g. still owe 100% of fees for remainder of term)
  - Institution should have the right to the return of its data after termination
  - Vendor should not have the right to either retain or destroy the institution's data
  - Clear wind-down and transition provisions and procedures for transitioning data back to institution or another vendor designated by institution

Business benefits of utilizing SaaS/cloud services (cont'd)

- **10) Insurance**
  - Cyber liability or other data breach insurance coverage is absolutely critical for these SaaS/cloud services
  - Also critical for institutions
  - Cyber liability is a very new line of insurance coverage, policy exclusions and carve-outs vary dramatically from carrier to carrier (and sometimes has high deductibles)
  - Also consider related business interruption due to cyber incidents
  - Courts starting to weigh in on what constitutes a "computer" incident, etc. – evolving case law on cyber liability policy interpretation

Emerging SaaS/cloud services issues regarding connected devices and Internet of Things (“IoT”)



Pre-computer Era

Wired Computing Era

Wireless Computer Era

Web of World/IoT

H2H

H2M

H2M

M2M

Emerging SaaS/cloud services issues regarding connected devices and Internet of Things (“IoT”)

- Huge and growing area
  - Of research and innovation
    - Connected/autonomous vehicles
    - Connected health devices
    - Smart home technologies
  - Of lawmaking and regulatory scrutiny
    - Remember: type of data collected/transmitted still triggers applicable law – HIPAA for PHI, GLBA for non-public personal information
    - Federal Trade Commission Activity
    - State law activity

Emerging SaaS/cloud services issues regarding connected devices and Internet of Things ("IoT") (cont'd)

- FTC Report "Internet of Things: Privacy and Security in a Protected World") https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

- Recommends a series of concrete steps that businesses can take to enhance and protect consumers' privacy and security, as Americans start to reap the benefits from a growing world of Internet-connected devices.

- Such devices offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits.

- However, the FTC report also notes that connected devices raise numerous privacy and security concerns that could undermine consumer confidence.

Emerging SaaS/cloud services issues regarding connected devices and Internet of Things (“IoT”) (cont’d)

- **State IoT Laws**
- Internet of Things Bill (CA SB 327); follows Connected Television Law of 2015
- Would require that any internet connected device provide reasonable security measures and clearly warn users when the device is recording audio or visuals or collecting information, including what type of information is collected (biometric, location and more).
- Could be first legislative mandate for IoT device manufacturers to proactively implement “**security by design**” (that is, at an early stage, and built into the product development process, rather than added reactively later as a “patch” or as an optional or voluntary industry best practice).
- Appears to be dead for this session (moved to “inactive” status as of June 1, 2017); massive industry and trade group opposition, including: CA Chamber of Commerce; CTA; Auto Alliance; Toy Association, and more.
- But don’t think this bill won’t be back in CA, or won’t arise in other states.

QUESTIONS?

Erin F. Fonté
Member

Payments, Fintech and Digital Commerce
Financial Institutions Regulatory & Compliance

Dykema
111 Congress Avenue, Suite 1800
Austin, Texas 78701
Direct: 512-703-6318
efonte@dykema.com
@PaymentsLawyer
LinkedIn Link me in: Erin Fonte

Cristina R. Blanton, J.D.
Associate Compliance Officer and Privacy Officer

Systemwide Compliance Office
The University of Texas System
201 West 7th Street
Austin, Texas 78701
Office: 512-852-3264
Fax: 512-579-5085

Follow us: **www.utsystem.edu**
@utsystem
UT System Facebook