Cloud Computing and Related Laws

Law Offices of
Salar Atrizadeh

When you think advocacy, think of us.®

Main Issues

- Online privacy (e.g., corporate and personal privacy)
- What are helpful policies to protect privacy?
- What is search engine privacy? What is social networking privacy?
- How does facial recognition software affect privacy?
- What is cloud computing? What are the different cloud services?
- How does virtualization and information technology outsourcing affect cloud computing?
- What is a "private cloud" and how does it affect privacy?
- What are the applicable state, federal, or international laws?

Online Privacy

In general, privacy falls under two categories:

1. Corporate privacy
2. Personal privacy

Corporate Privacy

- It concerns the protection of corporate data from retrieval or interception by unauthorized parties
- Security is important for protection of trade secrets, proprietary information, and privileged communications
- The failure to maintain confidentiality can result in a loss of "trade secret" status
- See *Civil Code §§ 3426 et seq*.

Corporate Privacy

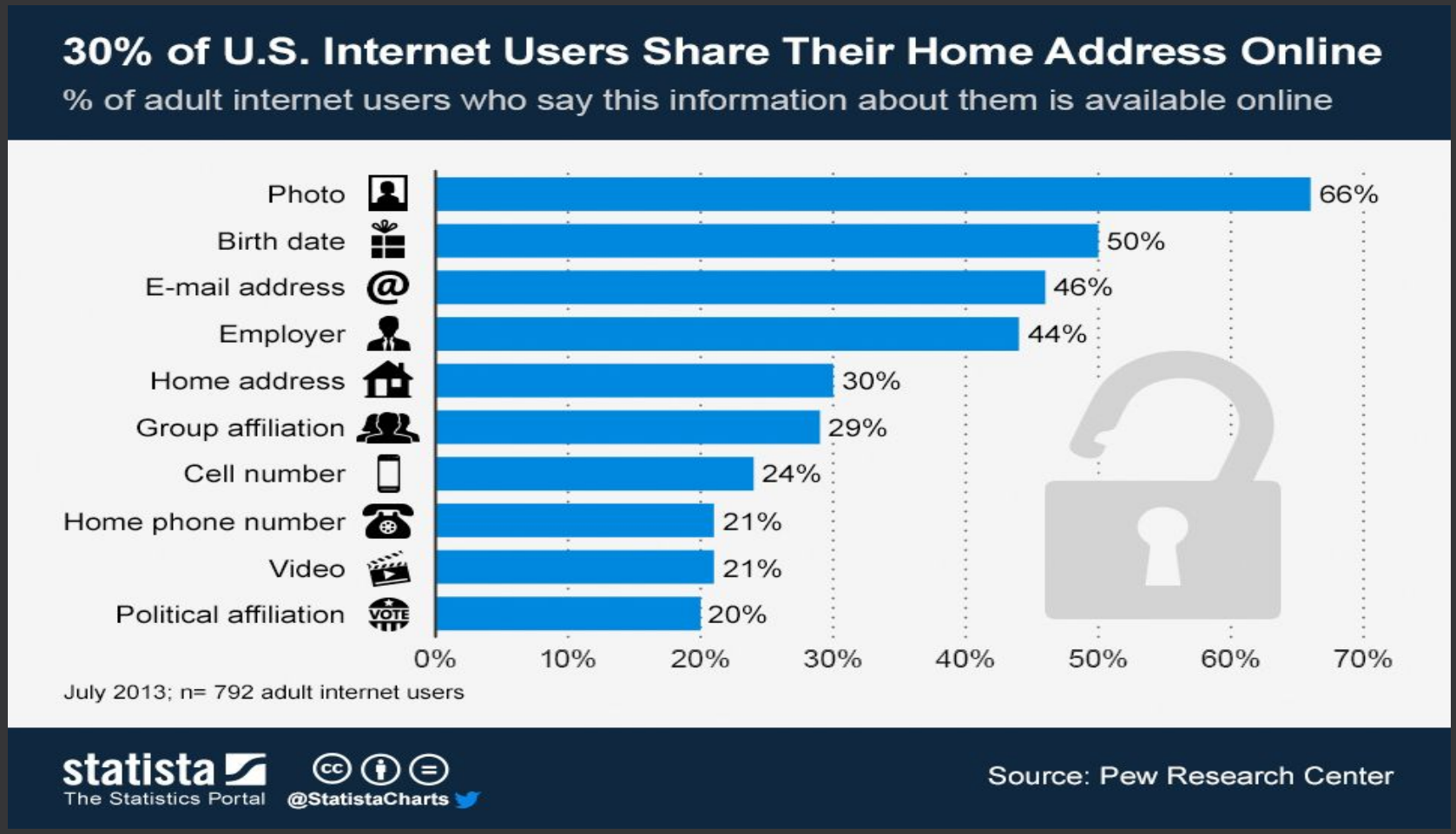
- The recent trends in outsourcing have increased the risks associated with "economic espionage"
- In fact, manufacturers should be cautious when transferring proprietary technology to overseas partners because foreign governments sponsor theft
- See 18 U.S.C. §§ 1831 et seq. (e.g., economic espionage, theft of trade secrets)
- See www.law.cornell.edu/uscode/text/18/1831

Helpful Policies

- Locate, identify, and label confidential information
- Restrict access to confidential information
- Use encryption – e.g., truecrypt.org, axantum.com
- Use firewall and secure username/password
- Use software that detects trade secret theft – e.g., safe-corp.biz
- Include warnings in privileged correspondence (e.g., "this email contains privileged communications")

Helpful Policies

- Provide computers without hard drives
- Prohibit use of removable storage (e.g., flash drives)
- Audit employee computers
- Prohibit and/or monitor external web-based email services
- Execute Confidentiality and Non-disclosure Agreements
- Execute Computer-Use Policies


30% of U.S. Internet Users Share Their Home Address Online
% of adult internet users who say this information about them is available online
Photo
66%
Birth date
50%
E-mail address
46%
Employer
44%
Home address
30%
Group affiliation
29%
Cell number
24%
Home phone number
21%
Video
21%
Political affiliation
20%
0%
10%
20%
30%
40%
50%
60%
70%
July 2013; n= 792 adult internet users
statista
The Statistics Portal
@StatistaCharts
Source: Pew Research Center

Personal Privacy

- Constitution
  - Federal: Fourth Amendment protects against unreasonable searches and seizures
  - State: California Constitution, under Art. I, § 1 recognizes right to individual privacy
- Federal computer crimes
  - Electronic Communications Privacy Act – 18 U.S.C. §§ 2510 et seq.
  - Privacy Act – 5 U.S.C. § 552a
  - Computer Fraud and Abuse Act – 18 U.S.C. § 1030

Personal Privacy

- Personal health/financial information
  - HIPAA – 42 U.S.C. §§ 1320d et seq.
  - Gramm-Leach-Bliley Act – 15 U.S.C. §§ 6801 - 6809
  - Fair Credit Reporting Act – 15 U.S.C. §§ 1681 to 1681u
  - Electronic Funds Transfer Act – 15 U.S.C. §§ 1693-1693r
- Common law
  - *Google, Inc. v. U.S.*, 95 Fed.Cl. 661 2011 WL 17619 (2014)
  - *Rene v. G.F. Fishers, Inc.*, 817 F.Supp.2d 1090 (2011)
  - *Amazon Web Services v. U.S.*, 113 Fed.Cl. 102 2013 WL 5952468 (2013)

Personal Privacy

- In today's world, cloud computing is risky because you can't secure its perimeter
- For example, state or federal agencies must comply with regulatory statutes (e.g., HIPAA, Sarbanes–Oxley Act)
- The National Institute of Standards and Technology compares adoption of cloud computing to wireless technology
- In recent years, organizations have learned how to protect wireless data, so they'll probably do the same with cloud computing

Personal Privacy

- Privacy rights can be waived by contract and privacy expectations may be negated by express policies
- Company's policies (whether formal or implied) may create a reasonable expectation of privacy ("REP") in electronic communications
- In general, users have REP in personal email contents and text messages
- See *U.S. v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007)

Personal Privacy

- "REP" depends on (a) person; and (b) context → sender of an electronic communication may not enjoy a REP under 4th Amendment once a message has been sent, even though the recipient may have one
- See *United States v. Lifshitz*, 369 F.3d 173, 190 (2nd Cir. 2004)
- A person has no legitimate expectation of privacy in information voluntarily turned over to a third party
- See *U.S. v. Jones*, 132 S. Ct. 945, 957 (2012)

Search Engine Privacy

- Search engines gather personally identifiable information
- What is it? See *Business & Professions Code § 22577*
- The information may include: (i) search terms; and (ii) time, date, location of the computer executing the search
- Risks:

  (a) behavioral marketing

  (b) public disclosure of personal information

  (c) Loss of privacy

Search Engine Privacy

- Question: Should search engines limit collection, retention, and disclosure of IP addresses (e.g., 129.244.100.245)?
- In the United States, federal law does not provide uniform privacy protections for personal data submitted to search engines or for IP addresses
- Federal regulations [e.g., 45 C.F.R. § 164.514(b)(O)] treat IP addresses as "individually identifiable" information for specific purposes (See ecfr.gov)

Search engines and privacy

CNET News.com posed a series of key questions on privacy practices to the leading search companies

	Data retained	Deleted or anonymized?	User info linked?	Behavioral targeting?	Opt out of BT?
Ask	Hours	Deleted	No	No	N/A
AOL	13 months	Deleted	No	Yes	Yes
Google	18 months	Partially anonymized	No	No	N/A
Microsoft	18 months	Deleted	Yes	Yes	No*
YAHOO!	13 months	Partially anonymized	Yes	Yes	No

**Can opt out of behavioral targeting on third-party sites but not MSN.com*

Source: News.com research

Social Networking Privacy

- What is a social networking website? An online forum that permits users to keep contact with friends and share personal information
- Risks v. Benefits:
  - Access by marketers, job recruiters, or government agencies
  - Employer access - Illinois Governor, Pat Quinn, signed a bill (i.e., Right to Privacy in Workplace Act) which prevents employers from demanding actual/prospective employees for social network usernames and passwords
  - Benefits – cyber omnipresence?

Facial Recognition Software

- In June 2012, Facebook announced its acquisition of Face.com, a facial recognition technology company
- Facebook uses an automatic facial recognition system, called "tag suggestions," to create a database of users' biometric information
- See bbc.com/news/technology-18506255

Facial Recognition Software

- Issues:

  i. Profile deletion mechanism - creating biometric profiles without users' consent lacks a clear profile deletion mechanism

  ii. Unauthorized access - Failing to implement safeguards to protect biometric information from unauthorized access

Facial Recognition Software

- A fear of crime and declining cost of hardware, bandwidth, and storage, are leading to the spread of technology for monitoring public spaces and identifying individuals
- Monitoring technologies, include, cameras, facial recognition software, and vehicle identification systems
- Facial recognition software is becoming more reliable
- See visionics.com and epic.org/privacy/facerecognition

Case Study: *EPIC v. FBI*

- FBI is developing a biometric identification database program called "Next Generation Identification"
- It'll be the largest biometric database in the world
- It aggregates fingerprints, DNA profiles, iris scans, palm prints, voice identification profiles, photos, and other identifying information
- On April 8, 2013, EPIC filed a Freedom of Information Act (under 5 U.S.C. § 552) lawsuit against the FBI to obtain documents
- See epic.org/foia/fbi/ngi

Cloud Computing

- Definition: A global technological infrastructure, where user of a computer accesses and uses software and data located outside of a digital device
- Scenario: A user connects to external devices thru an Internet connection, but has no knowledge of the nature/location of the server on which the data and software are located
- This anonymous, external, and often unidentifiable interaction is known as “cloud computing” or simply “the Cloud”
- See nist.gov/itl/csd/cloud-102511.cfm

What is cloud computing?

It refers to the use of computing power that is located elsewhere, in "*the cloud*" of remote networks

It's really just a name for storing and processing data online. For example, many of us already use cloud computing when using the internet for storing photos and emails.

WHERE'S MY DATA?
Data typically goes to large data centres in the network, depending on the type of cloud.

What are the different types of cloud?

PRIVATE
resource dedicated to one customer

PUBLIC
resources shared by multiple customers

HYBRID
customized combination of shared and dedicated resource

COMMUNITY
dedicated resource for a group of customers

What are the different cloud services?

SOFTWARE-AS-A-SERVICE
It enables a user to be able to use an application without installing it on a computer or other type of device.

PLATFORM-AS-A-SERVICE
It allows third parties to build applications without buying hardware or maintaining software.

INFRASTRUCTURE-AS-A-SERVICE
It provides hardware capacities as demanded by users, to run their own software services.

CLOUD SERVICES & EXAMPLES?

Microsoft Office 365 is a cloud-based software service offered to companies to improve productivity.

Start-ups like Zartis in the EU use the Windows Azure cloud-platform to develop their cloud-based apps that are then delivered to clients.

Swiss healthcare firm uses Microsoft Systems Center and Server to create and manage its own private cloud and services.

What are the benefits of cloud?

Improving efficiencies can result in savings of 80% of the costs of managing IT hardware.

Worldwide market for cloud services will be worth € 106.7 BN by 2014.

Cloud will add € 763 BN in productivity to the top economics over the next five years.

WHY ARE COMPANIES SHIFTING TO THE CLOUD?

- Cost effective
- Easy to Implement
- Secure & Reliable
- Flexible & Scalable
- Interoperable

For more information: www.microsoft.eu
www.microsoft.com/cloud

Microsoft

Types of services:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

IaaS

- It seeks to obviate the need for customers to have their own data centers
- The provider sells access to web storage space, servers, and internet connections
- The provider owns and maintains the hardware and customers rent space according to their needs
- The customer maintains control of software environment, but not over equipment
- Example: Amazon Web Services

IaaS

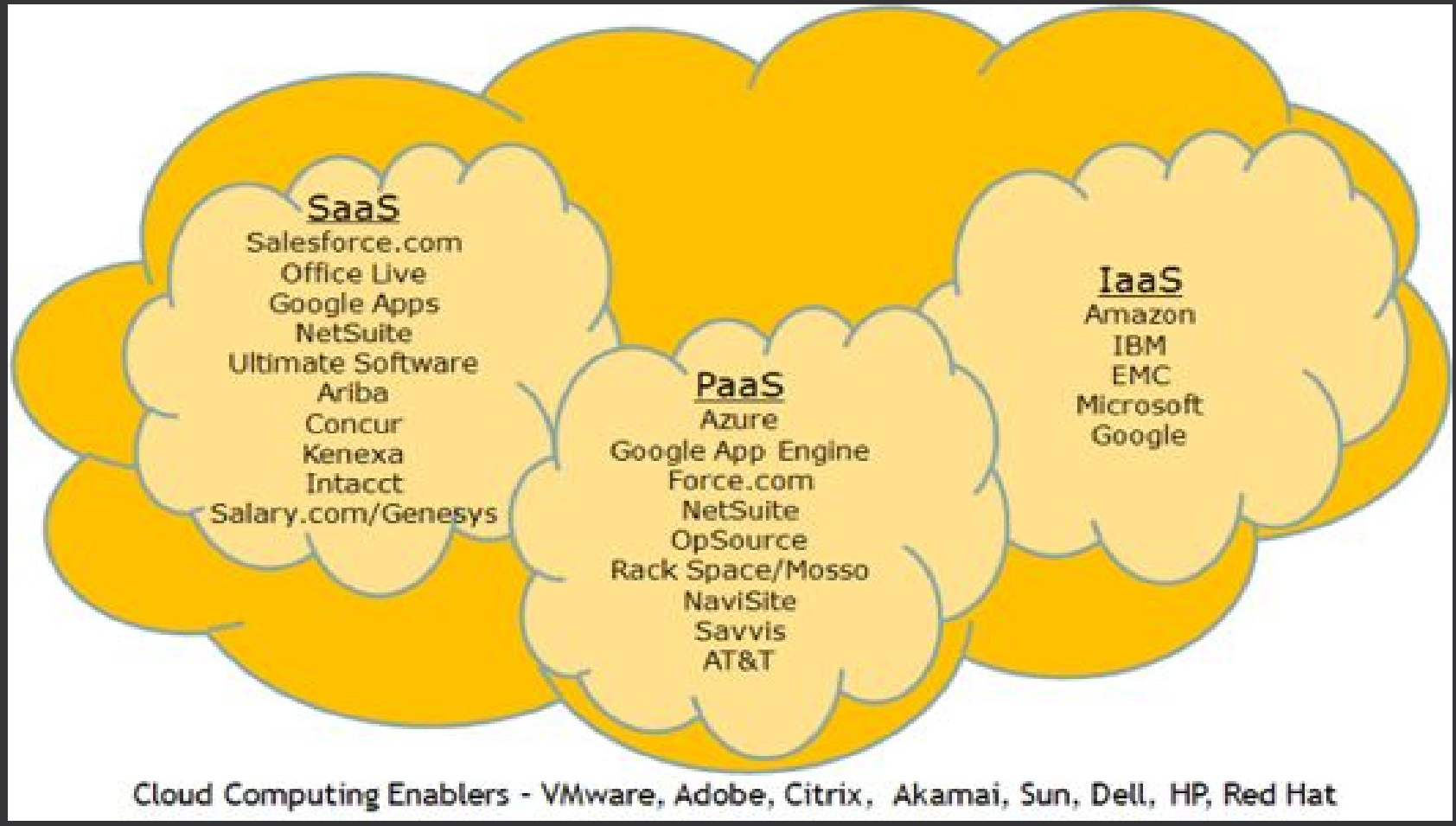
- The capability provided to the customer, includes, processing, storage, networks, and fundamental computing resources
- The customer is able to deploy and run arbitrary software (e.g., operating systems, applications)
- The customer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications

PaaS

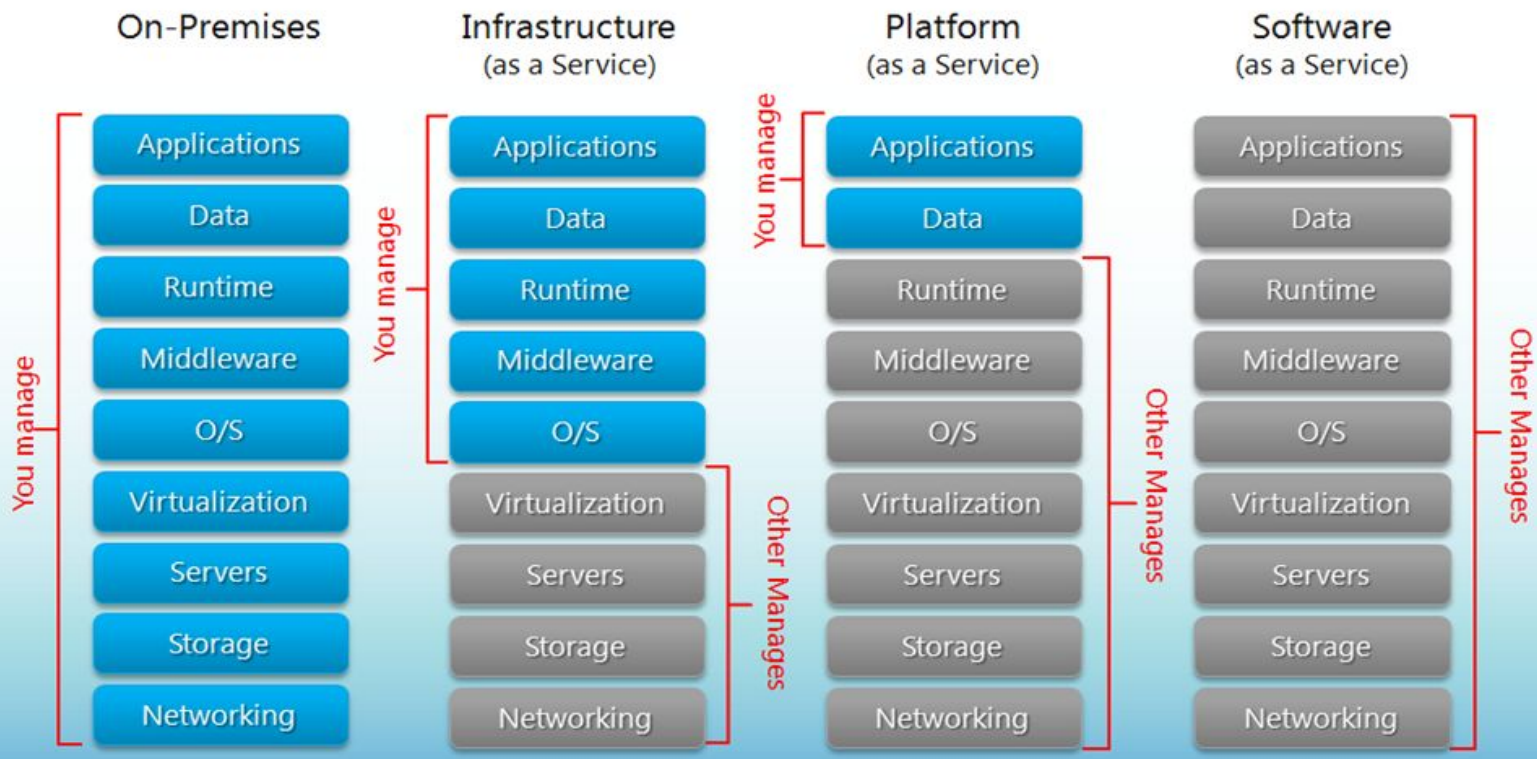
- It provides a place for developers to create and publish new web applications stored on provider’s servers
- The customers use the Internet to access the platform and create applications using the provider's API, web portal, or gateway software
- Examples: Saleforce's Force.com, Google App Engine, Mozilla Skywriter, Zoho Creator

PaaS

- It provides users with a computing platform
- The users can create, deploy, and host web applications
- The users maintain control over their applications and data
- The service providers deliver servers and system software
- It benefits software developers by getting rid of restrictions of limited computer capacity (e.g., processor speed, memory)


SaaS
Salesforce.com
Office Live
Google Apps
NetSuite
Ultimate Software
Ariba
Concur
Kenexa
Intacct
Salary.com/Genesys
PaaS
Azure
Google App Engine
Force.com
NetSuite
OpSource
Rack Space/Mosso
NaviSite
Savvis
AT&T
IaaS
Amazon
IBM
EMC
Microsoft
Google
Cloud Computing Enablers - VMware, Adobe, Citrix, Akamai, Sun, Dell, HP, Red Hat

Separation of Responsibilities



SaaS

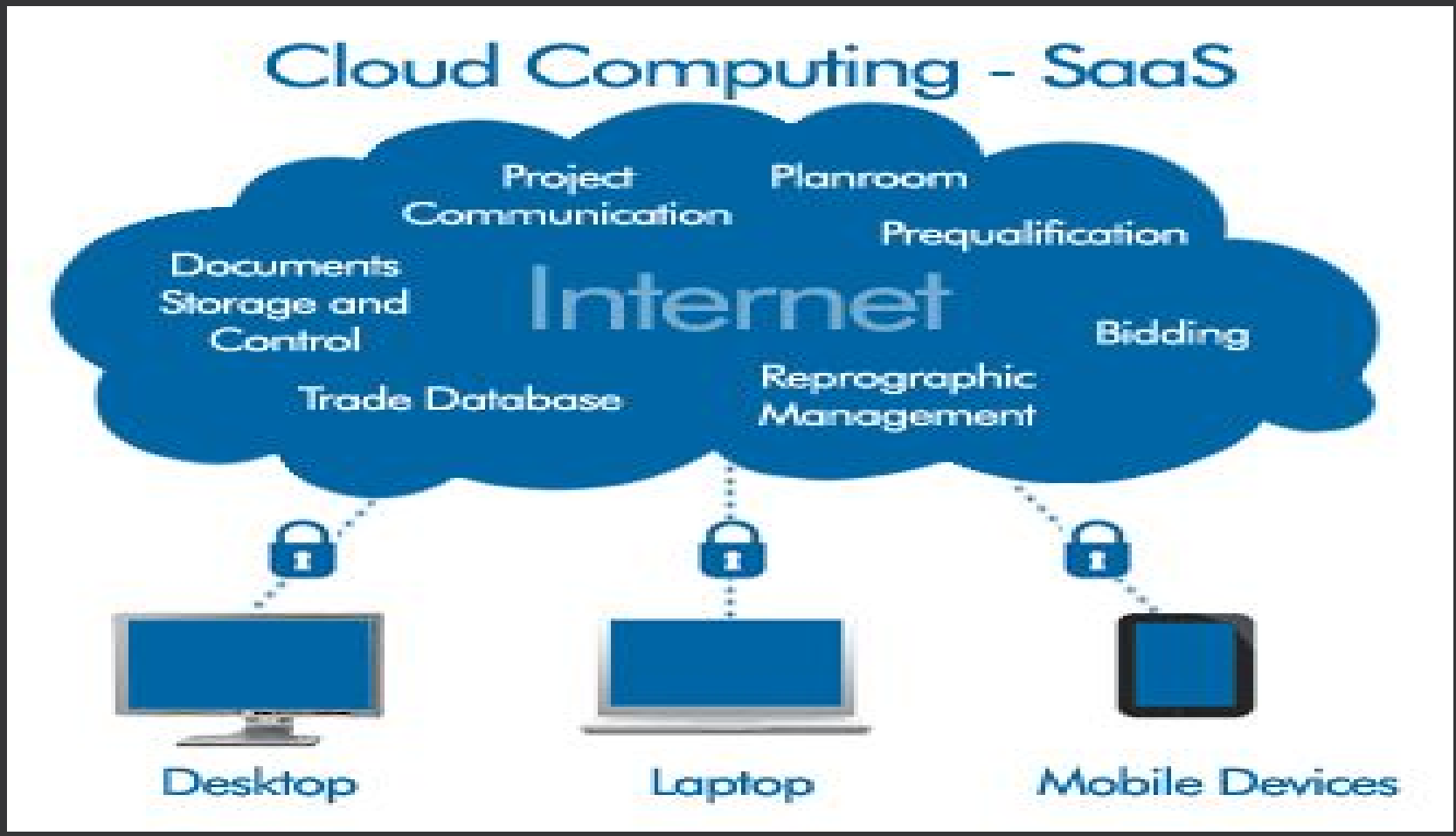
- It’s the most common service
- SaaS applications provide the function of software that would normally have been installed and run on the user's desktop
- The application is stored on the service provider's servers and runs through the user's web browser over the Internet
- Examples: Gmail, Facebook, YouTube

SaaS

- In SaaS, the processing happens in the “cloud”—outside of the user’s control
- The service provider manages infrastructure and software platforms
- The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email) or a program interface

SaaS

- The processing transpires in the “cloud” outside of the user’s control
- The service provider manages infrastructure and software platforms
- The user doesn’t manage/control the underlying cloud infrastructure (i.e., network, servers, operating systems, storage) with the exception of limited user-specific application configuration settings


Cloud Computing - SaaS
Project Communication
Planroom
Prequalification
Documents Storage and Control
Internet
Bidding
Trade Database
Reprographic Management
Desktop
Laptop
Mobile Devices

Cloud Computing

- In the SaaS model, the users access applications via a browser to add, review, sort and control data
- In the SaaS model, the custodian does not physically control data, so it's a complicated situation for litigation
- In the SaaS model, the client data is contained in a proprietary format that's controlled by the provider
- So, requesting data from these sources is costly and time consuming

Cloud Computing

- Social media is an example of the SaaS model
- The data created/stored on social media websites is stored on the provider's servers—which may/may not be the social media company itself—as it may outsource data storage and maintenance

Types of Cloud

- Public Cloud: When a cloud is made available in a “pay-as-you-go” manner to the general public
- Private Cloud: When a cloud is made available via an internal datacenter of a business or other organization
- Hybrid Cloud: When a public and private cloud are connected for sharing of data and applications

Internet of Things

- The Internet of Things (a/k/a “IoT”) is the next evolution and is making a remarkable impact on technology
- Devices are now able to communicate with each other through embedded sensors that are linked by wired and wireless networks
- For example, they include thermostats, automobiles, or pills that permit a physician to monitor the patient’s health

Internet of Things

- Technology advancements allow networks and objects they connect to become more intelligent
- The factors that are currently driving growth, include, development of smart cities, smart cars, and smart homes
- However, there are concerns with privacy and security
- Gartner predict that by 2020, more than 26 billion units will be connected to the Internet
- See gartner.com/newsroom/id/2684616

Internet of Things

- It's governed by information that's stored by devices without human intervention
- So, privacy may be compromised through various technologies
- See ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices
- Also, devices may not interact well due to development on incompatible platforms (i.e., lack of interoperability)

Internet of Things

- Wearable technology is able to generate constant, convenient, seamless, portable, and hands-free access to electronics and computers
- It can be used in the military, law enforcement, entertainment, and healthcare industries
- However, with every benefit comes a risk (e.g., violation of privacy rights)
- In *State v. McMurray*, 860 N.W.2d 686 (2015) the Supreme Court of Minnesota mentioned "Internet of Things" when Defendant moved to suppress narcotics evidence based upon a warrantless search and seizure of his trash

Internet of Things

- Drones (i.e., flying robots) are being used by military and non-military persons
- These flying robots, include, UAS and UAV, which are remotely-piloted autonomous systems
- These machines are useful for covert operations
- However, adapting to new devices has not been easy for society
- The major concerns are regulation, insurance, and privacy

Internet of Things

- Security is an important concern
- Devices are now able to interact with each other
- Devices can synchronize data with each other, which permits collaboration
- So, computer-controlled brakes, ignitions, locks and other automotive components are vulnerable

Internet of Things

- In order to adapt to this evolution, the legal system must concentrate on the interaction of information technology with other industries
- Our legal system must implement a uniform view to accommodate information technology
- Remote access allows criminals to obtain access to a network that contains confidential information (e.g., trade secrets)
- Other issues with remote access, include, data privacy, protection of proprietary rights, and liability for unauthorized use of systems

Internet of Things

- The Federal Trade Commission has held public workshops to explore consumer privacy and security issues posed by the growing connectivity of devices.
- The workshops focus on privacy and security issues related to connectivity for consumers—both at home (e.g., smart home appliances) and when consumers are mobile (e.g., fitness devices, personal devices, and automobiles).
- The European Union has also addressed the issues and risks (e.g., privacy, security, trust)

Virtualization

- Virtualization allows multiple computing resources (e.g., servers) to be hosted on one physical machine
- So, it permits a single server to behave as multiple servers
- Each of the virtual servers is called a “virtual machine”
- See webopedia.com/TERM/S/server_virtualization.html

Virtualization

- The benefits include:
  - Efficiency
  - Physical size reduction
  - Safer test environment
  - Easier disaster recovery
  - Enhanced compatibility with legacy systems
  - Enhanced security through separation of personal/business systems

Virtualization

- The risks include:
  - Unsecure/unencrypted communications
  - Unrestrained increase of virtual machines
  - Incompatibility and inoperability
  - Increased network strain
  - System crash

Virtualization

- The controls include:
  - Hypervisor maintenance
  - Secure/Encrypted communications
  - Change management
  - Pre-implementation testing
  - Disaster recovery planning

IT Outsourcing

- In today's business world, many companies outsource information technology procedures
- For example, they outsource: (1) cloud computing; (2) application development/maintenance; (3) infrastructure management; (4) help desk; (5) independent testing/validation; (6) data center management; (7) systems integration; (8) R&D; and (9) managed security

IT Outsourcing

The key questions when considering outsourcing are:

1. How do IT control activities that have been outsourced relate to business processes?
2. Are internal auditors properly involved in key stages of the outsourcing life cycle?
3. Do internal auditors have sufficient IT knowledge and experience to consider risk and provide the right input?

IT Outsourcing

4. If IT control activities are transitioned to an IT service organization, does it understand the roles and expectations of internal audit stakeholders?
5. Are internal auditors able to see IT risk and present recommendations for processes that have been outsourced?
6. What role do internal audit teams play during renegotiation, repatriation, and renewal of outsourcing contracts?

See GTAG 7, *Information Technology Outsourcing, 2nd Edition*

What is a Private Cloud?

- It permits clients greater control over the infrastructure and computational resources
- See *Peng, Zhang, et al., Comparison of Several Cloud Computing Platforms, Second International IEEE Symposium on Information Science and Engineering 23–27 (Dec. 26–28, 2009)*
- Department of Homeland Security is building a cloud platform for enterprise email and other services
- Also, Michigan and Utah plan to turn their IT departments into "private clouds" in order to provide resources to agencies

Privacy

- How can you protect personal information online?
- Examples of online activities are: (i) banking, (ii) emailing, (iii) sharing data
- Questions:
  - What happens to information when uploaded into the Cloud?
  - Where are passwords and account numbers saved?
  - Who can access them?

Privacy

- You should ensure a cloud service includes data encryption, effective data anonymization, and mobile location privacy
- In federal agencies, the contract with the service provider should include provisions for complying with the Privacy Act of 1974
- The location of a cloud provider's operations can affect the privacy laws that apply to the data
- Does your data need to reside within your legal jurisdiction?

Tips on protecting personal information:

1. Do not inadvertently reveal personal information
2. Turn on cookie notices in your browser or use cookie management software
3. Keep a "clean" e-mail address (e.g., private email account)
4. Avoid revealing personal details to unknown persons/entities

Tips on protecting personal information:

5. Avoid sending highly personal e-mail to mailing lists
6. Avoid replying to spammers
7. Be conscious of web security (e.g., https v. http)
8. Be conscious of home computer security (i.e., use firewall and encryption)
9. Examine privacy policies and seals (e.g., TRUSTe.com)

See consumer.ftc.gov

Contract Law

- In general, contract law is applicable to privacy rights
  1. Licensing Agreement - a contract where licensor gives licensee permission to use intellectual property
  2. End User License Agreement - contract between the licensor and purchaser that establishes purchaser's right to use software
- Question: Is there any equal bargaining power?
- So, who should have the power to collect, cross-reference, publicize, or share information about us?

Privacy Protection

Electronic Communications Privacy Act ("ECPA")

- Objectives:
  - To expand and revise federal wiretapping and electronic eavesdropping provisions
  - To support creation of new technologies by assuring safety of personal information for consumers
  - To protect electronic communications from unwanted interception by both state and private actors

ECPA

- It's codified under 18 U.S.C. §§ 2510-2522
- A violation may be punishable as a felony under 18 U.S.C. § 2511(4)
  - Violations/Remedies:
    - Individuals - up to 5 years imprisonment and a $250,000 fine
    - Victims are entitled to a civil suit of actual damages, punitive damages and attorney's fees
    - U.S. Government cannot be sued for a violation, but illegally-gathered evidence cannot be introduced in court

ECPA

- Title I - Wiretap Act
- Title II - Stored Communications Act
- Title III – Pen Register Act

Title I - Wiretap Act

- It's codified under 18 U.S.C. §§ 2510-2522
- Protects communications in transit
- Protects against both government and private intrusion into electronic communications
- The protection is strong in most situations
- Access requires a search warrant and any evidence obtained in violation of this part of the statute is subject to exclusion

Title II - Stored Communications Act

- It protects the storage of electronic information
- It covers nearly all information in the "Cloud" that is no longer in transit from sender to recipient (i.e., it refers to e-mails not in transit)
- There are exceptions for law enforcement access and user consent
- General rule: Employers are forbidden from accessing employee's private e-mails
- Exception: It may be lawful if consent is given in the form of an employment contract that explicitly authorizes access
- It's codified under 18 U.S.C. §§ 2701-2712

Title II - Stored Communications Act

- It distinguishes between a remote computing service (RCS) and an electronic communication service (ECS) provider, which have different standards of care
- In general, ECS providers offer the ability to send or receive wire or electronic communications [See 18 U.S.C § 2510(15)]
- It prohibits an ECS provider from knowingly divulging contents of any communication while in electronic storage [See 18 U.S.C. § 2702(a)(1)]
- It prohibits an RCS provider from knowingly divulging contents of any communication which is carried or maintained on that service

See *Crispin v. Christian Audigier* (C.D.Cal. 2010) 717 F.Supp.2d 965

Title III - Pen Register Act

- Pen Registers/Trap and Trace devices provide non-content information about the origin and destination of communications
- It's subject to less restrictions than actual content since it doesn't contain the communication's content
- U.S. Supreme Court
  - There is no "reasonable expectation of privacy" here because the telecommunication company already has access to it
  - The telecommunication company must utilize this information to ensure communications are properly routed/delivered

Title III - Pen Register Act

- There is no statutory exclusionary rule that applies when the government illegally uses a pen register/trap-and-trace device
- IP addresses and port numbers associated with the communication are fair game
- No private cause of action against the government
- It's codified under 18 U.S.C. §§ 3121-3127

ECPA: Disclosure of Records

- The ECPA lays out guidelines for law enforcement access to data
- Per the Stored Communication Act:
  - The government is able to access many forms of stored communications without a warrant (e.g., customer records)
  - Under 18 U.S.C. § 2703, a "National Security Letter" can be served to compel disclosure of basic subscriber information
  - Section 2703 allows a court to issue an order for records
  - Whether a "National Security Letter" or Court Order is warranted depends on the information

Type of Communication	Required for Law Enforcement Access	Statute
Email in Transit	Warrant	18 U.S.C. § 2516
Email in Storage on Home Computer	Warrant	4th Amendment, US Constitution
Email in Remote Storage, Opened	Subpoena	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for 180 days or less	Warrant	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for more than 180 days	Subpoena	18 U.S.C. § 2703

California Privacy Laws

1. Anti-Phishing Act of 2005 (Bus. & Prof. Code §§ 22948-22948.3) It prohibits "phishing" – i.e., posing as a legitimate company or government agency in an email, web page, or other internet communication – in order to trick a recipient into revealing his/her personal information.
2. Computer Spyware (Bus. & Prof. Code § 22947) – It prohibits an unauthorized person from knowingly installing or providing software that performs certain functions, such as taking control of the computer or collecting "personally identifiable information" on or to another user's computer located in California.

California Privacy Laws

3. Cyberbullying (Education Code § 32261) – It defines "bullying" as one or more acts of sexual harassment, hate violence, or intentional harassment, threats, or intimidation, directed against school district personnel or pupils, committed by a pupil or group of pupils. Bullying includes a post on a social network website and is a ground for suspension or expulsion.
4. Online Privacy Protection Act of 2003 (Bus. & Prof. Code §§ 22575-22579) – It requires operators of commercial websites or online services that collect personal information on California residents through a website to conspicuously post a privacy policy on their website and to comply with it.

California Privacy Laws

5. Personal Information Collected on Internet (Gov. Code § 11015.5) – It applies to state government agencies. When collecting personal information electronically, agencies must provide certain notices and prior to sharing someone's information with third parties, they must obtain written consent.
6. Public Officials (Gov. Code § 6254.21) – It prohibits posting or displaying the home address or telephone number of any elected or appointed official (on the web) if the official has made a written demand not to disclose his/her information.

Fair Information Practice Principles

i. Notice/Awareness - to individuals about information collected, maintained, and used by the entity

ii. Choice/Consent – consumers must be able to "opt-in" and "opt-out"

iii. Access/Participation – it gives individuals access to information and the ability to correct mistakes

iv. Integrity/Security – the administrative, technical and physical safeguards of the information and notice of data breaches

v. Enforcement/Redress - legal, policy, contractual, or ethical

See ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

Cloud Computing Act of 2012

- Proposed by Senator Amy Klobuchar (D-MN) - September 19, 2012
- It attempts to give "cloud computing services" extra protections under the Computer Fraud and Abuse Act (CFAA)
- It states that each instance of "unauthorized access" (the lynchpin of liability under the CFAA) of a cloud computing account is a separate offense
- Loss is presumed to be the greater of the value of the loss of use or information, or a minimum of $500, multiplied by the number of accessed cloud computing accounts
- See http://beta.congress.gov/bill/112th/senate-bill/3569/text

Computer Fraud and Abuse Act ("CFAA")

- Is a hybrid civil-criminal law - See 18 U.S.C. § 1030
- It originally passed as a purely "anti-hacker" criminal statute prohibiting wrongful access to computers
- It focused on issues relating to the protection of federal computers and financial institutions. It also touched on interstate and foreign cybercrimes
- The 2002 amendment (a/k/a "Patriot Act") gives federal officials flexibility on monitoring and prosecuting suspected cybercriminals
- It' also been used by employers for internal data breaches and misappropriation by employees

Any Questions?

Salar Atrizadeh, Esq.
Law Offices of Salar Atrizadeh
9701 Wilshire Blvd., 10th Floor
Beverly Hills, CA 90212
T: 310-694-3034
F: 310-694-3057
Email: salar@atrizadeh.com
Website: www.atrizadeh.com
Blog: www.internetlawyer-blog.com