Flying Instruments-Only
Navigating Legal & Security Issues in Cloud Computing

Richard P. Goldberg
Attorney at Law
(and former Java architect)
DISCLAIMER:

Richard.Goldberg@GoldbergLawDC.com

@GoldbergLawDC (twitter)
Richard.Goldberg@GoldbergLawDC.com
I am a lawyer.

I am not your lawyer.
(except some of you, and you already know who you are)
Cloud computing is dangerous
“In the event of a crash landing, put your head between your legs...”

“...and kiss your ass goodbye.”
“You can delegate authority, but you can never delegate responsibility.”

— Richard E. Krafve

General Manager,
Ford Motor Company,
Edsel Division
What are the risks?
What are the risks?
Are you protected?
What are the risks?
Are you protected?
What can you do?
What is cloud computing?
cloud computing (n): _
Promise
Secure data
Secure replicated data
No more backup tapes
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Multitenancy
Third-Party Admin
Automatic
Automatic scaling
Automatic scaling
Are all of these cloud?
Probably not
It doesn’t matter
The things that are cloud...
and...
and...
The things that just look like cloud...
The things that just **look** like cloud...

... have the **same** problems
2 things create problems in cloud computing
Multitenancy
Third-Party Possession
This is not the problem
It's this
You can’t say civilization don’t advance... in every war, they kill you in a new way.

— Will Rogers
Why is cloud risky?

“Man does not control his own fate. The women in his life do that for him.”

— Groucho Marx
Why is cloud risky?

“Man does not control his own fate. The women in his life do that for him.”

— Groucho Marx
Control
Transparency
Transparency vs. Control
So what’s the worst that can happen?
“Dear Google Docs user . . . .

We’ve identified and fixed a bug which may have caused you to share some of your documents without your knowledge.”
0.05%

4.4 million users

2,200 users

0.05%
4.4 million users
x 0.05% = 2,200 users

... or 30 times the total number of Twitter employees
T-Mobile

- Estimated one million customers lose data
- Customers wait two weeks for it to be restored
- Data is two weeks old
Voicemail transcripts from Google voice appear in Google search results.

Google knows but doesn’t tell anyone.
“He who knows does not speak.”
— Lao Tzu
“He who knows does not speak.”

— Lao Tzu
“He who knows does not speak.”

— Google
“He who knows does not speak.”

— Google

(and Toyota)
Why did it take so long?
We’ll get to that...
QuickBooks online failure

Financial data unavailable for over 6 hours

No explanation provided to customers

February 2009
June - July 2010

- Complete data-center failure
- Financial data unavailable for over 24 hours
- Followed by rolling failures over 4 weeks
- Directed customers to Twitter for updates
More failures bring down customer sites

Some fixed in 2 hours, others last half a day

Experts blame DOS attack, Intuit stays quiet
How can you know?
How can you know?

Control and Transparency
Data Breaches by year

- 2004: 24
- 2005: 141
- 2006: 533
- 2007: 490
- 2008: 717
- 2009: 441
- 2010: 499+
64% of data breaches originate outside the organization

Source: Open Security Foundation
When a data breach involves a **third party**...
twice as many records are stolen

Source: Open Security Foundation
Many attacks originate outside our walls.
Are we all moving to cloud?
In a survey by Symantec of Senior VPs, VPs, and Directors of 2010 priorities...
...cloud computing ranked 13th after energy savings
So what are we doing here?
In a survey by Gartner of Chief Information Officers of 2010 priorities...
cloud computing ranked 2nd after virtualization
What does that mean for cloud computing?
The future of cloud is uncertain
The market is fractured
There's no turning back
Still, there is a problem...
Cloud Computing...

You can only test it once: after you jump

- the height of the bridge
- the length of the rope
- if the rope is made of rope
- if the rope is connected to anything but your ankles
You can’t see this until...
Careful, the beverage you are about to enjoy may be very hot.

CUP CONTAINS 10% POST-CONSUMER RECYCLED FIBER
Inherent Dangers
Inherent Dangers

Service Agreements
Inherent Dangers
Service Agreements
Collateral Dangers
Inherent Dangers
Service Agreements
Collateral Dangers
Solutions (if any)
Inherent Dangers
Inherent Dangers
Federal Data Protection Laws
HIPAA
Health Insurance Portability and Accountability Act
“Business Associate Agreements”
encryption vs. onerous data breach reporting
“Reasonably anticipated threats or hazards”
FIPS 140-2
& SP 800
More federal laws are coming
Rep. Bobby Rush (D-IL) (he survived)

Data Accountability and Trust Act
Passed the House of Representatives
December 8, 2009

a day after a day that will live in infamy
Mirrors protections in Gramm-Leach-Bliley Act
Requires consumer and FTC notification after data breach
...unless “no risk of harm”
Preempts existing state law
We’ll get to that...
Sen. Patrick Leahy (D-VT) → Personal Data Privacy and Security Act
“This [bill] . . . provide[s] Americans with notice when they have been victims of a data breach . . . [and] also deals with the underlying problem of lax security . . . to help prevent data breaches from occurring.”

— Sen. Patrick Leahy
Sen. Patrick Leahy (D-VT) times 3
It’s not just the feds...
It’s not just the feds...

45 states and D.C.
Some are less strict than others...
Some are less strict than others...

“A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.”

— Utah Protection of Personal Information Act
Utah Code § 13-44-202
... and some are more strict.
“Every person . . . Shall . . . [e]ncrypt[] all transmitted records and files containing personal information that will travel across public networks, and . . . all data containing personal information to be transmitted wirelessly . . . [e]ncrypt[] all personal information stored on laptops or other portable devices . . . there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.”

— Massachusetts Data Breach Protection Act
M.G.L. c. 93H; 201 CMR 17.03
“there must be reasonably **up-to-date** firewall protection and **operating system security patches**”
Some level of **security**

Notification upon breach
Added requirements for **certain data** if there is a breach
International Data Protection Laws
European data privacy laws are strict.

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

— U.K. Data Protection Act
Requires employee consent
Requires employee consent
Requires employee consent

informed
Requires employee consent

revocable
not enough
EU Data Protection Directive
“right to be forgotten”
Streamlined international data transfer
Corporate Data Policies
Payment Card Industry (PCI) Data Security Standard
Audits?

Mind if we look around?

Hello, 911? We’d like to report an intruder...
Meet standard or face steep fines
Attorney-Client Privilege
Reasonable Precautions
Reasonable Precautions
Reasonable Precautions
Reasonable Precautions
Reasonable Precautions?
Subpoena
Civil Discovery

Federal Rule of Civil Procedure 34(a)(1)

“to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control . . . any designated documents or electronically stored information . . . stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form”
Issued by the
UNITED STATES DISTRICT COURT
District of Columbia

Someone Who Had An Idea

V.

Sucker, LLC

SUBPOENA IN A CIVIL CASE

Case Number: 1 2:07-cv-65535 (S.D.N.Y.)

TO: Poor Schlub
12345 Combination Idiot Would Have On Luggage Ln, Washington, D.C. 20005

☐ YOU ARE COMMANDED to appear in the United States District court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY

COURTROOM

DATE AND TIME

☒ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

DATE AND TIME
02/07/2010 10:00 a.m.

☒ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):

All correspondence and/or documents memorializing communications between you and any officer, manager, partner, member, or employee of Sucker, LLC regarding the idea we had and you stole.

PLACE
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

DATE AND TIME
02/07/2010 10:00 a.m.

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES

DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rule of Civil Procedure 30(b)(6).

ISSUING OFFICER’S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)

DATE
3/5/2008

ISSUING OFFICER’S NAME, ADDRESS AND PHONE NUMBER

(See Federal Rule of Civil Procedure 45 (c), (d), and (e), on next page)

1 If action is pending in district other than district of issuance, state district under case number.
<table>
<thead>
<tr>
<th>PLACE OF TESTIMONY</th>
<th>COURTROOM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DATE AND TIME</td>
</tr>
</tbody>
</table>

☐ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

DATE AND TIME
02/07/2010 10:00 a.m.

☐ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):
All correspondence and/or documents memorializing communications between you and any officer, manager, partner, member, or employee of Sucker, LLC regarding the idea we had and you stole.

PLACE
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

DATE AND TIME
02/07/2010 10:00 a.m.

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES

DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rule of Civil Procedure 30(b)(6).

ISSUING OFFICER’S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)

DATE
3/5/2008

ISSUING OFFICER’S NAME, ADDRESS AND PHONE NUMBER

(See Federal Rule of Civil Procedure 43 (c), (d), and (e) on next page)
You are commanded to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

Place of Deposition
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

Date and Time
02/07/2010 10:00 a.m.

You are commanded to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):
All correspondence and/or documents memorializing communications between you and any officer, manager, partner, member, or employee of Sucker, LLC regarding the idea we had and you stole.

Place
Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500

Date and Time
02/07/2010 10:00 a.m.

You are commanded to permit inspection of the following premises at the date and time specified below.

Premises

Date and Time

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rule of Civil Procedure 30(b)(6).

Issuing Officer's Signature and Title (Indicate if Attorney for Plaintiff or Defendant)

Date
3/5/2008

Issuing Officer's Name, Address and Phone Number

(See Federal Rule of Civil Procedure 45 (c), (d), and (e), on next page)

If action is pending in district other than district of issuance, state district under case number.
**PLACE OF TESTIMONY**

<table>
<thead>
<tr>
<th>COURTROOM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DATE AND TIME</th>
</tr>
</thead>
</table>

**YOU ARE COMMANDED** to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

**PLACE OF DEPOSITION**

<table>
<thead>
<tr>
<th>Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DATE AND TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/07/2010 10:00 a.m.</td>
</tr>
</tbody>
</table>

**YOU ARE COMMANDED** to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):

All correspondence and/or documents memorializing communications between you and any officer, manager, partner, member, or employee of Sucker, LLC regarding the idea we had and you stole.

**PLACE**

<table>
<thead>
<tr>
<th>Law Office of Richard P. Goldberg, 1600 Pennsylvania Ave. NW, Washington, DC 20500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DATE AND TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/07/2010 10:00 a.m.</td>
</tr>
</tbody>
</table>

**YOU ARE COMMANDED** to permit inspection of the following premises at the date and time specified below.

**PREMISES**

<table>
<thead>
<tr>
<th>DATE AND TIME</th>
</tr>
</thead>
</table>

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rule of Civil Procedure 30(b)(6).

**ISSUING OFFICER'S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)**

<table>
<thead>
<tr>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/5/2008</td>
</tr>
</tbody>
</table>

**ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER**

As used herein, the term “documents” shall mean and include, without limitation, the original and all copies of any written and any other tangible thing including the following: any handwritten, typed, oral, visual, or electronic communications or representations, agreements, contracts, letters, envelopes, correspondence, e-mails, telegrams, facsimiles, bulletins, calendars, circulars, notices, specifications manuals, instructions, directives, guidelines, meeting minutes, working papers, accounts, literature, books magazines, newspapers, articles, press releases, trade letters and internal and external newsletters, questionnaires, booklets, work assignments, reports, motion picture films, videotapes, advertisements, brochures, sound recordings, photographs, drawings, charts, graphs, diagrams, studies, analyses, surveys, memoranda, memoranda of conversations, notes, notebooks, diaries, data sheets, telephone logs, telephone messages, work sheets, calculations, drafts of the aforesaid, computer-readable data, and all copies of the aforesaid upon which have been placed any additional marks or notations, in your possession, custody, or control. Any documents contained in electronic storage, such as on computer diskette or any other computer-readable form, shall be produced in that same form.
A litigation hold to freeze data
Can you ensure files won’t be deleted?
Have "deleted" files been deleted?
Are they on a backup tape you don’t control?
Data retention policies may leave sensitive data lingering around.
You may have to produce it
This guy is bad enough
What if it’s this guy?
What if an employee is paying bribes?
What if an employee is paying bribes?
Two options:
(both are bad)
Why?
Transparency
Third-Party Possession
Multitenancy
Cloud Service Provider Agreements
“The best way to keep one’s word is not to give it.”

— Napoleon
“4.2 You acknowledge and agree that the form and nature of the Services which Google provides may change from time to time without prior notice to you.”
“4.3 . . . you acknowledge and agree that Google may stop (permanently or temporarily) providing the Services . . . to you or to users generally at Google’s sole discretion, without prior notice to you.”
“4.4 You acknowledge and agree that if Google disables access to your account, you may be prevented from accessing the Services, your account details or any files or other content which is contained in your account.”
“12.1 You will not have access to your data stored on the Rackspace Cloud™ during a suspension or following termination.”
“12.2 We backup the Rackspace Cloud systems.

... we may destroy all but the most recent backup. These backups may not be available to you.”
Cloud provider agreements tend to protect the cloud provider.
Not the cloud consumer
Trust
Trust
Faith
Trust
How?
We’ll get to that...
Collateral Dangers
“To expect the unexpected shows a thoroughly modern intellect.”

— Oscar Wilde
“To expect the unexpected shows a thoroughly modern intellect.”

— Oscar Wilde

“There are also unknown unknowns—the ones we don’t know we don’t know.”

— Donald Rumsfeld
Third-Party Subpoena
Federal Rule of Civil Procedure 45(a)(1)(A)(iii)

“command each person to whom it is directed to do the following . . . produce designated documents, electronically stored information, or tangible things in that person’s possession, custody, or control”
...and here
Is data properly segregated?
This is more than just a data leak...
it's a disaster
Who will get the first call?
What do you do with old backups?
Third-Party Subpoena

Federal Rule of Civil Procedure 45(a)(1)(A)(iii)

No notice requirement.
Third-Party Subpoena
*Federal Rule of Civil Procedure 45(a)(1)(A)(iii)*

No notice requirement.

If a cloud provider gave up your sensitive data...
Third-Party Subpoena

Federal Rule of Civil Procedure 45(a)(1)(A)(iii)

No notice requirement.

You would never know
It's a disaster
Third parties want your data.
Google wants to index your data.

All of it.
You would never know
You would never know

Control and Transparency
“Probable cause”
Fourth Amendment Search Warrant
“Specific and articulable facts . . . the data is relevant and material”

Stored Communications Act
§ 2703(d) Order
“Specific and articulable facts . . . the data is relevant and material”

Stored Communications Act
§ 2703(d) Order

SCA requires “prior” notice
Notice can be postponed 90 days
So what’s the real danger?
How bad can it get?
Cloud computing is dangerous
Cloud computing is dangerous.
Cloud computing is dangerous

And the plane
I am Richard P. Goldberg

We are not related
Uses your cloud service provider...
The FBI can back up a truck...
...and seize everything
“They confiscated everything, even the stuff we didn’t steal.”
No
No comment
future?
FBI Defends Disruptive Raids on Texas Data Centers

(Crydon Technology and Core IP)

FBI agents seized about 220 servers belonging to him and his customers, as well as routers, switches, cabinets for storing servers and even power strips.

Customers who went to... try to retrieve their equipment were threatened with arrest.

“The trouble with heart disease is that the first symptom is often hard to deal with: *sudden death.*”

— Dr. Michael Phelps
Solutions (if any)
“On the Internet, nobody knows you’re a dog.”

Enhance Transparency
Los Angeles Goes Google

As of Monday, city employees will be able to start using Google Apps for daily computing tasks . . .
Cloud computing will evolve.
“Yes, he’s a sleazy lawyer, but he’s my sleazy lawyer.”

Increase Control
Control and Transparency
But how?
Trust
Advance notice of data release
Encryption
Prompt notice of data breach
Clear data-retention policies
Audit rights
Rights to access data
But there are still problems
You need a plan in advance
Failure to notify
Failure to adhere to policies
No employee vetting
Data seizure or service failure
Company counsel must understand these issues
before an emergency
Not your audience
It may feel like this
Change the Law
(and the landscape)
CloudAudit/A6

Automated Audit, Assertion, Assessment, and Assurance API

(This attacks the transparency problem.)
Digital Due Process
Electronic Communications Privacy Act Reform

(This attacks the control problem, but only for law enforcement.)
Coalition for Platform Parity

Search Warrant, Subpoena, and Border Search Reform

(This attacks the control problem.)
Reform requires support

(Without it, some current problems cannot be solved.)
A quick summary...
“You can delegate authority, but you can never delegate responsibility.”

— Richard E. Krafve
General Manager,
Ford Motor Company,
Edsel Division
This guy
This guy
Uses your cloud service provider...
“They confiscated everything, even the stuff we didn’t steal.”
Control
Transparency
Third-Party Possession
Multitenancy
Cloud provider agreements tend to protect the cloud provider
Trust
Change the Law
(and the landscape)
Cloud computing is dangerous
Cloud computing is dangerous

And the plane
Flying Instruments-Only
Navigating Legal & Security Issues in Cloud Computing

Richard P. Goldberg
Attorney at Law
(and former Java architect)

@GoldbergLawDC (twitter)
Richard.Goldberg@GoldbergLawDC.com