

Thinking Cloud Services – Look Before You Leap



Brian V. Cummings
brian.cummings@tcs.com
Tata Consultancy Services

Friday, March 16, 2012
Session 10358



Visit www.SHARE-SEC.com
for more information on
the SHARE Security &
Compliance Project

Preamble

*Cloud security literature consistently boils down
to one repetitive message:*

Don't put any important information in the Cloud!

What The Cloud Looks Like to Proponents



What the Cloud looks like to Security folks



Or, Maybe this!



What does it really look like?

The reality is mixed
Some things to applaud
Some things that worry
One big thorny issue



What Cloud are we talking about?

- The concept of cloud computing dates to the 1960's
- Cloud computing comes in a number of forms, deployments,
- Bottom line:
Our “Cloud” concern is where your data sits in any external environment that is under someone else's management, and the concern increases to the extent the resources in that environment are shared across the provider's clients.

What do Cloud Providers tell us?

- Cloud Providers will tell you
 - Security is best in class
 - Your data is safe
 - The benefits of cloud will set you free...



Who owns the responsibility

Owners vs Custodians

Cloud service consumers (Owners) cannot shift responsibility for information security or disaster recovery to a cloud provider.

Cost and execution can be shifted. Consumers can leverage services provided by the provider, and enhance the capabilities.

Cloud provider has custodial responsibilities which vary depending on the type of cloud service.

Cloud Security Concerns

Identities

Authentication

Passwords

Privacy

Data

Identities and Authentication

- Once it was only a label
- It was deemed “public” information, expected to be known
- Man in the middle and hijack attacks necessitated changes
- The concept of an identity and its authentication is changing
 - An account name
 - A device
 - A user selected icon or picture
 - Out of band confirmation
 - Email confirmation

Identities: Facebook Device

Name New Device

Please give this device a name. Because you have Login Notifications enabled, you will receive a notification that you logged in from this machine.

Device name:

Save Device

Don't Save

Identities: Facebook Confirmation

Facebook login from "TCS PC"



Inbox x



Facebook notification+zj4oj9=6=sa6@facebc
to me ▾

6:40 PM (3 minutes ago) ☆



Hi Brian Cummings,

A new device named "TCS PC" logged into your Facebook account (Thursday, March 15, 2012 at 6:40pm) from San Antonio, TX, US (IP=12.7.236.253). (Note: This location is based on information from your ISP or wireless provider.)

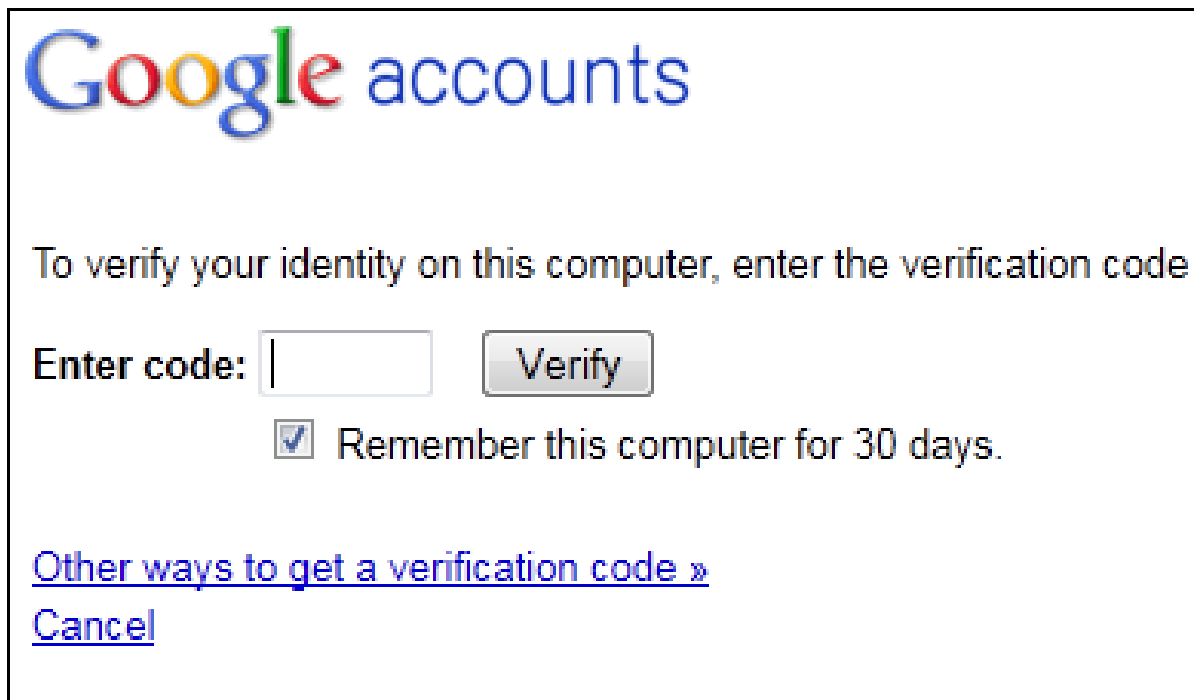
This device has been added to your account.

Was this you? If so, you can disregard the rest of this email.

If this wasn't you, please follow the link below to protect your Facebook account information:

<https://www.facebook.com/checkpoint/checkpointme?u=100002797187456&n=MYtEf8B0>

Authentication: Google 2-Step



Google accounts

To verify your identity on this computer, enter the verification code

Enter code:

☒ Remember this computer for 30 days.

[Other ways to get a verification code »](#)

[Cancel](#)

Cloud-Based Identity Management

[Identity Management - SailPoint Named a Leader in IAG.](#)
www.sailpoint.com/2011GartnerMQforIAG
Download the Analyst Report Today.

[Identity Management | IdentityManagement.com](#)
www.identitymanagement.com/
Easy to deploy Workflow-Powered **Identity Management** & Self-Service

[Cloud SSO & Provisioning | intel.com](#)
www.intel.com/go/identity
Analyst Reports, Video Tutorials, Free Trial from Intel

[Identity Management Companies To Demonstrate Simple Cloud ...](#)
www.sailpoint.com › [News & Events](#) › [Press Releases](#) › [Archive](#)
Oct 18, 2011 – **Identity Management Companies** To Demonstrate Simple **Cloud Identity Management** (SCIM) Specification at Internet Identity Workshop (IIW) ...

[Secure Cloud Identity Management | Ping Identity](#)
pingidentity.com/
Ping Identity delivers single sign-on and **identity management**, increasing IT security and ... Ping Identity® — The **Cloud Identity Security Leader** ... RSA 2012: eWEEK Labs Picks the 21 Hottest Security **Vendors**- 29 February 2012, eWeek ...

[News for cloud identity management vendors](#)
[Identity management in the cloud emerges as hot-button issue for CIOs](#)
[Network World](#) - 4 days ago
Sallie Mae uses **identity management** software from SailPoint to ensure that its 6100 ... of whether it's stored in the **cloud** or at one of its data centers.

[IETF explores new working group on identity management in the cloud](#)
www.networkworld.com/.../030912-identity-management-ietf-25710...
6 days ago – A specification already exists for Simple **Cloud Identity Management**

[NetApp® Cloud Computing](#)
www.netapp.com/cloud
Thinking **Cloud**? Think NetApp Storage. Watch Video to See Why!

[Identity Management Suite](#)
www.hitachi-id.com/
Manage user lifecycle securely and efficiently

[Identity Management](#)
www.oracle.com/identity
Leaders Quadrant Gartner MQ Report for User Provisioning. Download Now

[Microsoft® Private Cloud](#)
www.microsoft.com/readynow
Microsoft® Private **Cloud**: Built for the Future. Get Info on Resources!

[IAM in the Cloud](#)
www.courion.com/identity-mgt-cloud
Access **Management** in the **Cloud Identity Management Cloud** Solution

[Identity Management](#)
www.fischerinternational.com/
Simple and Easy IdM: easy roll-out, provisioning GUI, no programming.

[Identity Cloud](#)
www.symplified.com/Free-Asset-Download

Ads - Why these ads?

Internet 100%

Passwords

- Self-Service password selection and change
- Strong password enforcement
- Coupled with extended identity authentication
- Other considerations
 - Enforce periodic changes
 - Ability to use a different password for sensitive services
 - Password reverification
 - Cloud-based password management and single sign-on

**Buyer Beware:
Not all providers enable user password change!**

Google Application Passwords



Google - Reverification



Accounts

Why do I need to enter my password ?

To help protect your privacy, we'll sometimes ask you to verify your password even though you're already signed in.

Verify

Google

Email

bvcummings@gmail.com

Password

••••••••

Verify

[Can't access your account?](#)

[Sign out and sign in as a different user](#)

Cloud-Based Single Sign-On

Ads - Why these ads?

[NetApp® Cloud Computing - Thinking Cloud? | NetApp.com](http://www.netapp.com/cloud)

www.netapp.com/cloud

Think NetApp Storage. Watch Video to See Why!

Solutions for the Private Cloud - Private Cloud and Cloud Services

[Single Sign-On Solutions - Preferred, Secure SSO Solutions.](http://www.imprivata.com/GartnerReport)

www.imprivata.com/GartnerReport

Get Free Gartner SSO Vendor Report!

[Free Gartner Hype Cycle | intel.com](http://www.intel.com/go/identity)

www.intel.com/go/identity

For Identity and Access Management Technologies. Immediate Download.

[Cloud Single Sign-On & Federated Identity](https://www.pingidentity.com/.../SSO-and-Federated-Identity.cfm)

<https://www.pingidentity.com/.../SSO-and-Federated-Identity.cfm>

Internet SSO, as the name implies, is **single sign-on** that works across the Internet . It allows users with Web browsers to securely access multiple Web ...

[Single sign-on for the cloud and SaaS - OneLogin](http://www.onelogin.com/)

www.onelogin.com/

As I looked to extend our security perimeter to the **cloud**, I wanted a solution that provided the requisite control, while still seamlessly existing in Netflix's Freedom ...

Login - Company - Downloads - Product

[Intel announces Cloud SSO beta program](http://www.networkworld.com/news/.../022712-intel-cloud-ss0-256621.ht...)

www.networkworld.com/news/.../022712-intel-cloud-ss0-256621.ht...

Feb 27, 2012 - Intel today announced the availability of a **cloud-based single sign-on (SSO)** authentication and authorization service under a beta program ...

[Intel Launches Cloud SSO Beta Program](http://www.crn.com/news/.../intel-launches-cloud-ss0-beta-program.htm)

www.crn.com/news/.../intel-launches-cloud-ss0-beta-program.htm

Feb 27, 2012 - Intel has launched the beta program for **Cloud SSO**, a service that

Ads - Why these ads?

[Cloud Single Sign-On](http://www.okta.com/)

www.okta.com/

Single Sign-on for all web apps, on premise, SaaS, SAML, or proprietary

[Single Sign-On Made Easy](http://www.janrain.com/)

www.janrain.com/

Single Sign-On For Your Online Ecosystem. Easy To Implement

[Enterprise Single Sign On](http://www.onesite.com/)

www.onesite.com/

Easy to implement **Single Sign On** Integrate all your sites and apps

[Cloud Solutions](http://www.symplified.com/Avail-Free-Download)

www.symplified.com/Avail-Free-Download

Keep Your Data & Identities Safe with Simplified **Cloud** Solutions.

[Secure Internet SSO](http://www.pingidentity.com/)

www.pingidentity.com/

Ping Identity Management=Security For Proven **Cloud** Security Access

[Unified Single Sign On](http://www.sutisoft.com/sutisecure/)

www.sutisoft.com/sutisecure/

Manage your web application credentials with a **Single Sign On**

[Enterprise Single Sign-On](http://www.sutisoft.com/sutisecure/)

Internet 100%

Privacy – Google Privacy Policy

- **Information we collect**
- We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online. We collect information in two ways:
- **Information you give us.** [Personal information](#), [Google Profile](#),
- **Information we get from your use of our services.**
 - **Log information**
 - **Device information**
 - **Location information**
 - **Unique application numbers**
 - **Local storage**
 - **Cookies and anonymous identifiers** (Google services)

Privacy – Customer Control

- Privacy Principles
 - Customer should have full control over the selection of privacy settings.
 - Customer should have the option to opt out of user experience data collection.
 - Customer should be able to review, correct, delete any information collected and stored for an account.
 - Email confirmation of changes in any account settings
 - For social media, notifications when anyone posts, writes, pokes, or otherwise touches your account and information

Buyer Beware:
Sign on to services only for selected activities.

Data Security

Google Information Security Statement

Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using [SSL](#).
- We offer you [two step verification](#) when you access your Google Account, and a [Safe Browsing feature](#) in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

Information Security Thorny Issue

Infrastructure Security

Minimal security: Access control

If client data is comingled on storage devices or in databases, how is client data segregation assured?

How is data protected from “abuse of privilege” by infrastructure folks.

How is your data protected on portable media or remote storage for archive or backup purposes?

Information Security - Encryption

Infrastructure Security

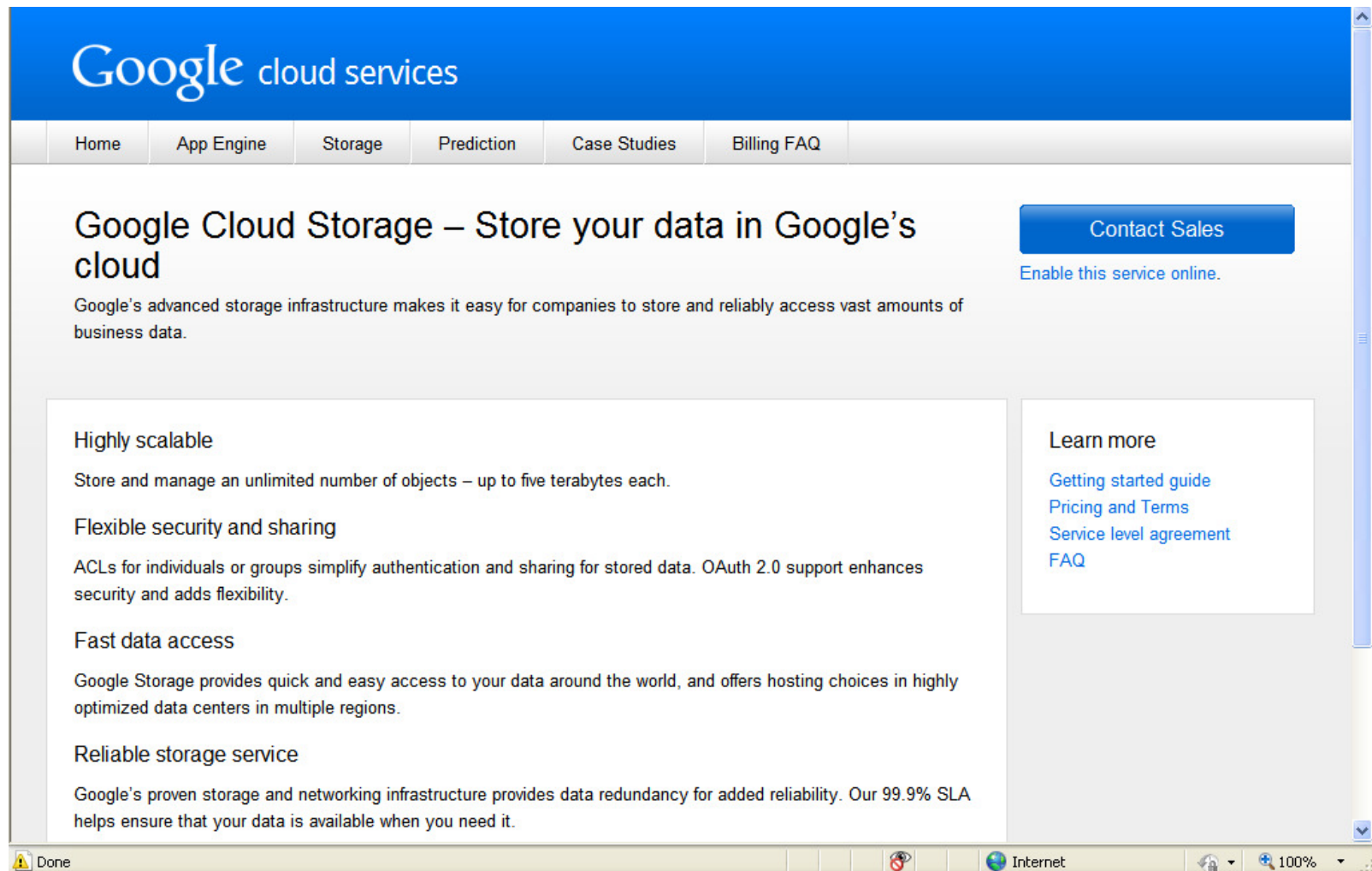
Cloud providers typically do not offer encryption.

Too many issues

- *Client by client, or full encryption of all customer storage?*
- *Who manages the keys?*
- *What is the legal liability?*

Customers will need to implement encryption

Google Enterprise Storage Encryption



The screenshot shows the Google Cloud Storage website. At the top is a blue header with the "Google cloud services" logo. Below the header is a navigation bar with links: Home, App Engine, Storage, Prediction, Case Studies, and Billing FAQ. The main content area features the heading "Google Cloud Storage – Store your data in Google's cloud" and a "Contact Sales" button. Below the heading is a paragraph about Google's advanced storage infrastructure. To the right of the main text is a "Learn more" section with links to "Getting started guide", "Pricing and Terms", "Service level agreement", and "FAQ". The bottom of the page shows a browser window with a "Done" button and a "100%" zoom level.

Google cloud services

Home App Engine Storage Prediction Case Studies Billing FAQ

Google Cloud Storage – Store your data in Google's cloud

Google's advanced storage infrastructure makes it easy for companies to store and reliably access vast amounts of business data.

[Contact Sales](#)
Enable this service online.

Highly scalable

Store and manage an unlimited number of objects – up to five terabytes each.

Flexible security and sharing

ACLs for individuals or groups simplify authentication and sharing for stored data. OAuth 2.0 support enhances security and adds flexibility.

Fast data access

Google Storage provides quick and easy access to your data around the world, and offers hosting choices in highly optimized data centers in multiple regions.

Reliable storage service

Google's proven storage and networking infrastructure provides data redundancy for added reliability. Our 99.9% SLA helps ensure that your data is available when you need it.

Learn more

- [Getting started guide](#)
- [Pricing and Terms](#)
- [Service level agreement](#)
- [FAQ](#)

Done Internet 100%

Cloud Provider Attestation

About SherWeb

[Company](#) |
 [Team Members](#) |
 [Partners](#) |
 [Why SherWeb](#) |
 [Distinctions](#) |
 [Testimonials](#) |
 [News](#)

Your data, now in even better hands

Ensuring our clients' peace of mind is critical to our success. After all, business email and related information is highly sensitive and all business activities should strictly comply with industry standards. That's why we take a proactive approach to ensuring the security of our customers' mission-critical data.

To guarantee the safest hosting environment possible, we recently improved our data safeguards by successfully completing the SAS 70 Type II audit.


Performed by Deloitte, one of the world's leading professional services firm, this audit goes well beyond the SAS 70 Type I audit. In addition to certifying that we have developed and implemented standard controls to manage our business and the delivery of our service to customers, the SAS Type II audit certifies that these controls are properly designed and rigorously applied at all times.

What is SAS 70?

The Statement on Auditing Standards 70 (SAS 70) is a widely-recognized accounting

Why is SAS 70 Type II important?

Service providers are required to implement

Done


Cloud Security Summary

Identities – need cloud federation



Authentication - extended



Passwords – strong passwords
required



Privacy – full customer control



Data – encrypt sensitive data

The End! Thank you!

Questions?



The Minions of Despicable Me