

CONTEXTUAL PRIVACY – REDEFINING PRIVACY FOR THE PERPETUALLY CONNECTED WORLD

Chenxi Wang, Alvin Tan
McAfee

Security in
knowledge



Privacy in a connect world



Seattle Reign FC @SeattleReignFC

47 mi

Imagine: an in-stadium app for Glass. Fan videos, pics & comments plus real-time stats, polls & analysis from Seattle Reign FC

[#ifihadglass](#)



Will M @Zenbyo

Feb 20

[#ifihadglass](#) there would be no more cheating on my **food** log :o It would also make it a lot easier to record weight loss efforts.



conradschulman @conradschulman

Feb 23

[#ifihadglass](#) I would wire the [#glass](#) to find parking using an image recognition api that displays open spots nearby.
pic.twitter.com/S56pShil3E

Privacy violations abound



Invasion of something, comes with a nice list of bars to never go to!

San Francisco Bars to Install Creepy Facial Detection Cameras Inside Venues – San Francisco News – T
blogs.sfweekly.com

Last year, San Franciscans were pretty freaked out when they learned that some of their favorite watering holes had...

Like · Comment · Share

WHAT THEY KNOW | October 13, 2012

When the Most Personal Secrets Get Outed on Facebook

Article

Slideshow

Comments (292)



By GEOFFREY A. FOWLER



Lance Rosenfield/Prime for The Wall Street Journal

Taylor McCormick was outed after he was added to a Facebook group that automatically informed friends he had joined a choir, *Queer Chorus*, at the University of Texas, Austin.

Why do these problems occur?

Privacy Notice

This Notice provides information about data we use for security purposes and our commitment to using the personal data we collect in a respectful fashion.

[Go here for our complete notice.](#)

McAfee Privacy Notice

McAfee and its family of companies ("McAfee", "we", "us") are wholly owned subsidiaries of Intel Incorporated. We care deeply about your privacy and security and your safety is a significant part of our essential mission. We appreciate your decision to trust us with helping to protect your digital life from theft, disruption, and unauthorized access to your personal information and systems.

This privacy notice is designed to inform you about how your personal information is collected, managed, and used to:

- Safeguard devices and data
- Manage our relationship with you
- Improve security products and services to predict future vulnerabilities
- Protect data

By collecting and processing data, we can help to predict threats and protect you, your devices and your information. McAfee is committed to becoming as transparent as possible to help you understand how your data is processed, why it takes data to protect data, and our commitment to using the personal data we collect for the purposes discussed in this Notice. Every time you turn on a device, connect to a network or open a file, you face significant risk from hackers, spammers, malware, spyware and other forms of unauthorized access to your data. This is why it is important to use security products and services such as McAfee's.

To defend against these threats and the thousands of new threats that emerge each day, McAfee technologies may:

- Analyze data sent to your devices for signs of risk or suspicious activity in order to take corrective action
- Assess the reputation of the sending device to determine whether access should be allowed or if the transaction should be continued;
- Adapt responses to new threats based on intelligence from our global network.

— Other factors

- ▶ It's difficult for companies to know what to do
 - ▶ Regulations are complex & they change frequently
- ▶ With mobile, more personal information is at stake
 - ▶ The possibility for abuse and misuse is high
- ▶ Consumer, Marketers, IT, and privacy advocates have different notions of “privacy”
 - ▶ Who is right?

So how do we
realistically tackle
this problem?



— Privacy is deeply contextual

- ▶ Privacy should be assessed under a certain context
 - ▶ Information shared under one context should not be treated the same under a different one
- ▶ Example:
 - ▶ I shared my “location” info with an airline app on travel days, but not otherwise.

Context is everything

— What is “context”

- ▶ Temporal
 - ▶ This activity will end at *<time>*
- ▶ Spatial
 - ▶ I am currently at *<location>*
- ▶ Application/usage
 - ▶ I use this service for *<purpose>*
- ▶ Functional/identity
 - ▶ I engage in this activity as *<role>*
 - ▶ I interact with this *<business>*
- ▶ Social
 - ▶ I undertake this activity with *<entity>*



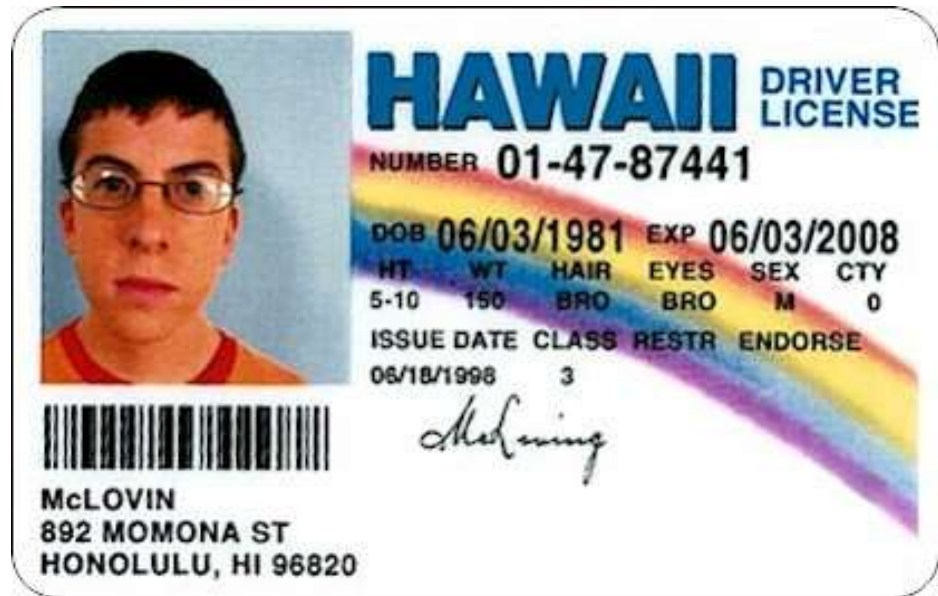
— An example

- ▶ A traveler may consent to share his location info on the day of the travel with a hotel app
 - ▶ But he would like to withhold that information from the app otherwise
 - ▶ Temporal & application context
- ▶ How to implement this?
 - ▶ A calendar app on the phone shares location with the hotel app only for the day of travel



— An example in the physical world

- ▶ A guy walks into a bar
 - ▶ What information does he minimally disclose?
 - ▶ He is over the legal drinking age (18 in Singapore)
 - ▶ He is at this location at this time
 - ▶ His gender



Continue this example





- ▶ Minimal context – Answer the question
 - ▶ “Are you over the legal drinking age?”
- ▶ Consider this – you walk into a bar
 - ▶ A camera takes your picture and sends to a cloud service
 - ▶ The service responds with – “Yes” or “No”
 - ▶ The picture is erased immediately
- ▶ This achieves the highest privacy

— What about marketers?

- ▶ Marketers may want more:
 - ▶ Your contact info – send your promotions
 - ▶ Age/gender – assess promotional efforts
 - ▶ Location info – track your likes and dislikes

What if we have a convention?

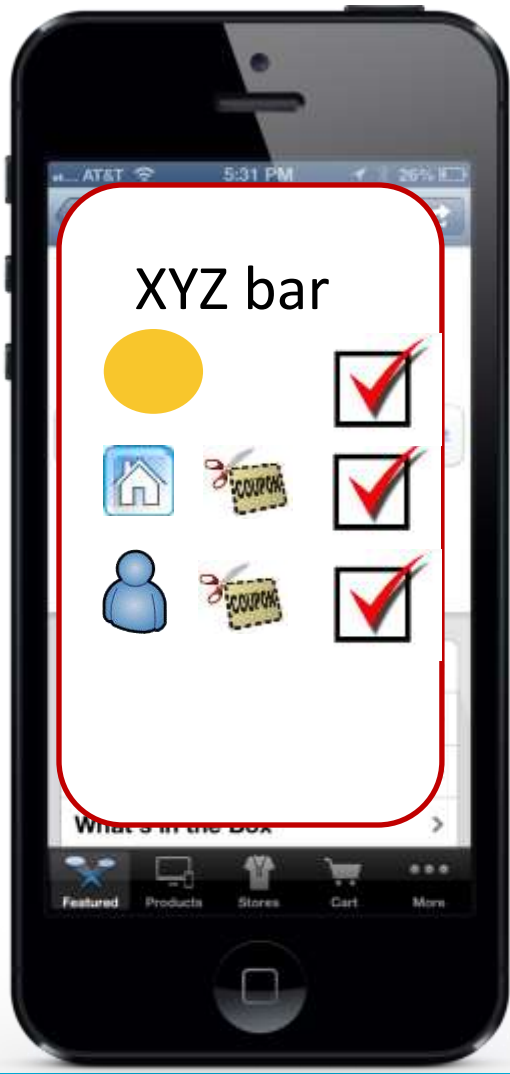


Symbol	Meaning
	Minimal context, nothing else.
	We collect <u>contact info</u>
	We collect <u>demographic info</u>
	We collect <u>location info</u>





— What about this model?



← Share info for coupons


— Why is this good?

- ▶ No complicated privacy policies
- ▶ Minimal context option is there
- ▶ Transparency

- ▶ Consumer desire & organizational requirements need not be at odds with each other
 - ▶ Consumers are given the choice to reveal minimal context
 - ▶ Or decide to share more

- ▶ Hypothesis – Consumers will share more with this model

Let's see a real use case

 **McAfee**
An Intel Company

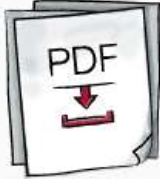
Privacy Notice

Your safety is our business

Thanks for trusting us to help protect your digital life from theft, disruption, and unauthorized access to your personal information and systems. This Notice provides more information about data we use for security purposes and our commitment to using the personal data we collect in a respectful fashion.


Read the full text version of the Privacy Notice here:

Follow the McAfee Privacy Ninja for a guided explanation:




DOWNLOAD TEXT PDF

and



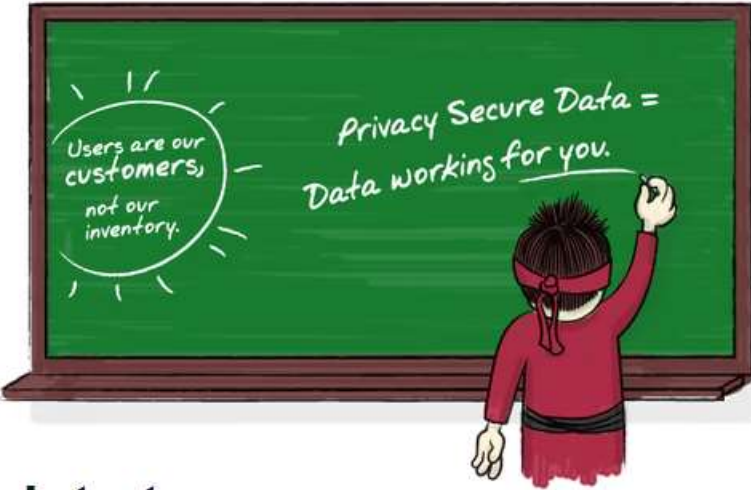
LET US SHOW YOU AROUND

 Listen to Privacy Notice





<http://www.mcafee.com/common/privacy/english/index.htm>

McAfee's privacy Ninja

McAfee & Data



We use data to:

-  Safeguard devices and systems
-  Manage our relationship with you
-  Improve security products and services
-  Protect Data







PREVIOUS NEXT

We might collect data

Collect & Use

When you give it to us, we collect your personal and non-personal data

We collect your personal information when you or someone acting on your behalf provides it to us. We also collect information when you obtain or use McAfee products, services or when you communicate with a device using McAfee's services.

-  Contact Information
-  Payment Information
-  Shipping and Billing Address
-  Purchase History
-  Username and Password
-  Communications with Us

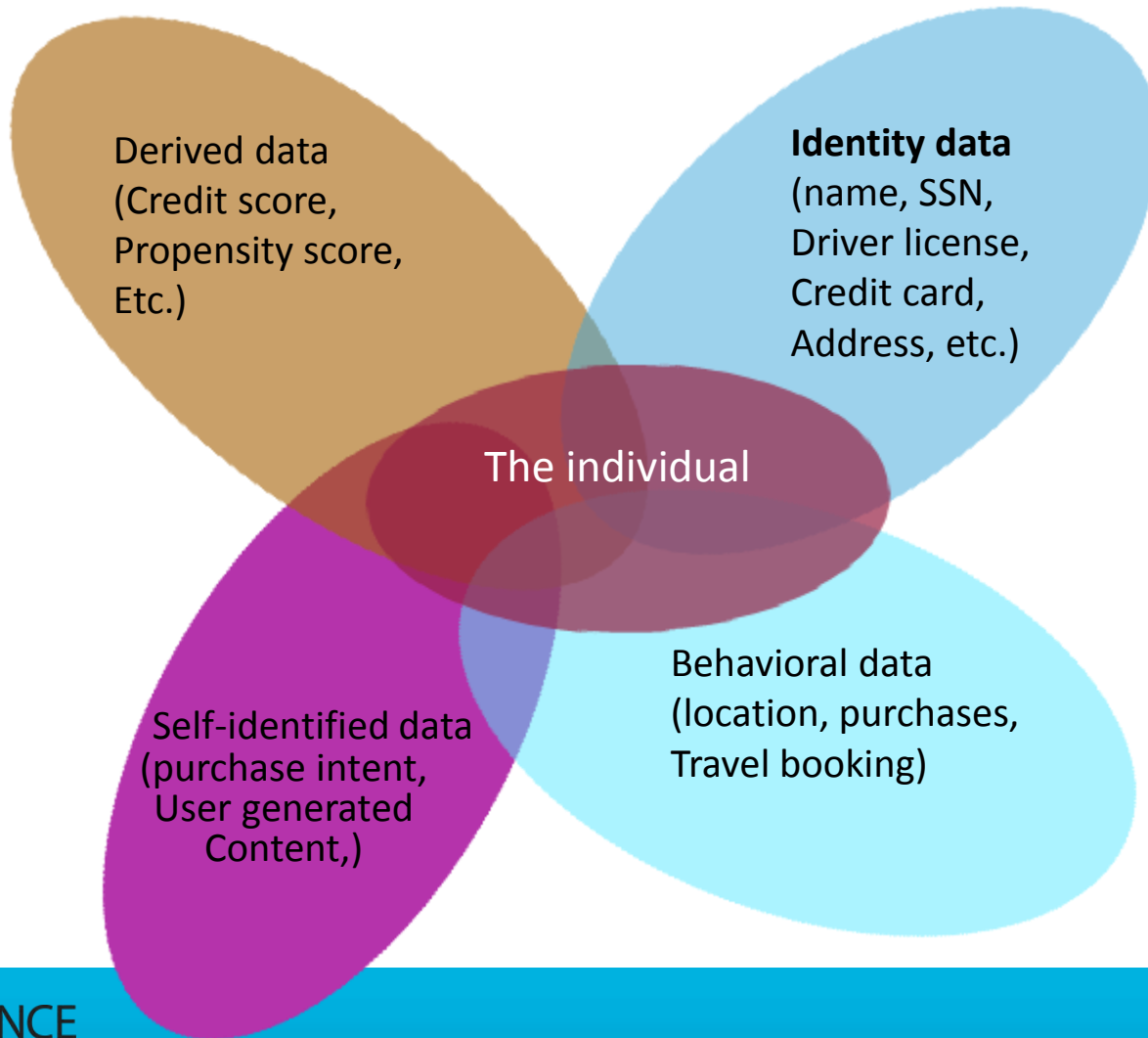
We might collect...

Details about your computers, devices, applications and networks (including IP address, browser characteristics, device ID and characteristics, device operating system information and system language preferences);

← →

PREVIOUS NEXT

A more general data framework



— Adding application context

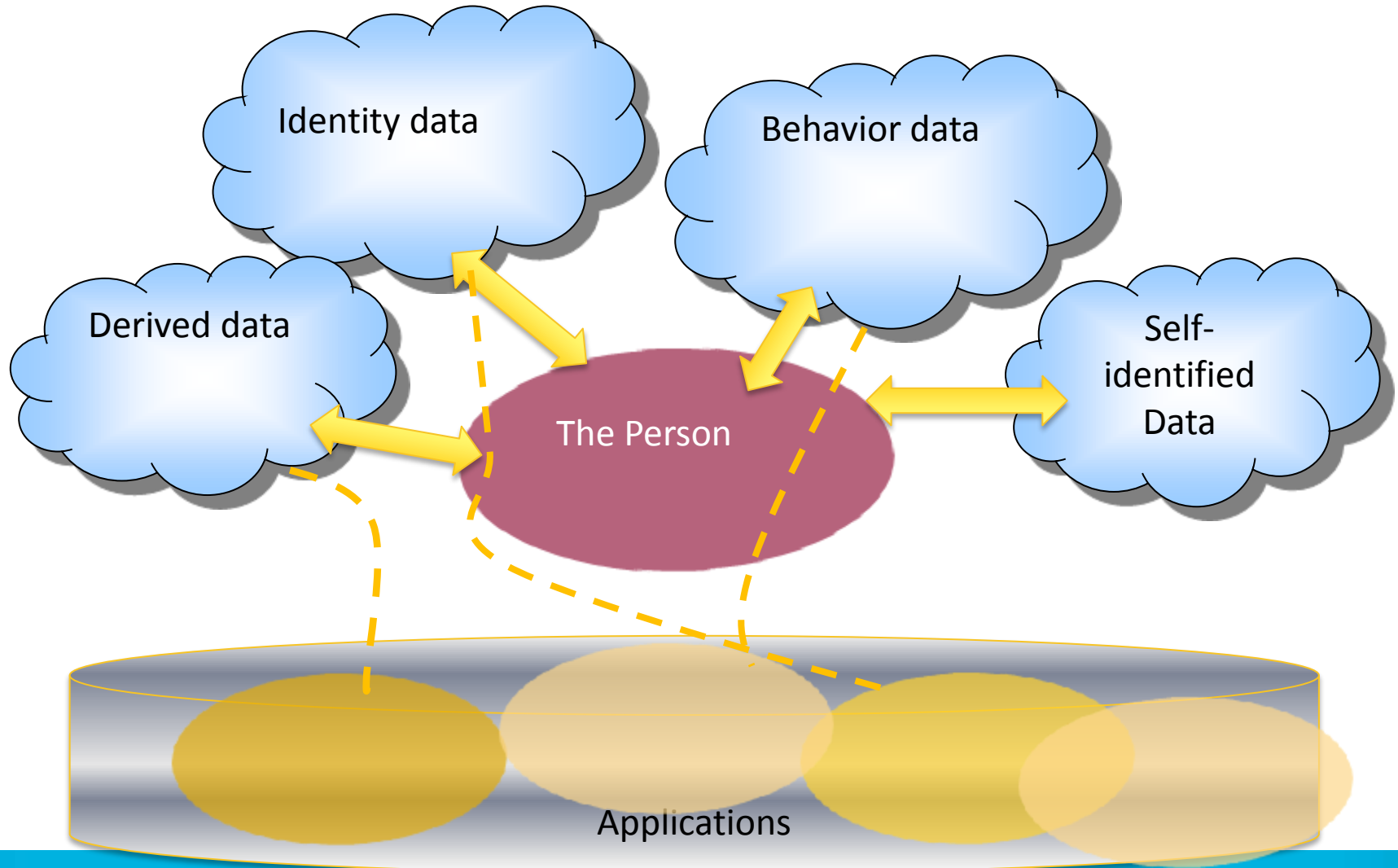
- ▶ <Research my next vacation>
 - ▶ Make info from my last 5 trips available for the travel agent app
 - ▶ Beyond my trip, data is no longer shared

- ▶ <Navigation>
 - ▶ Share my location info only
 - ▶ No marketing, no data mining, no third party sharing

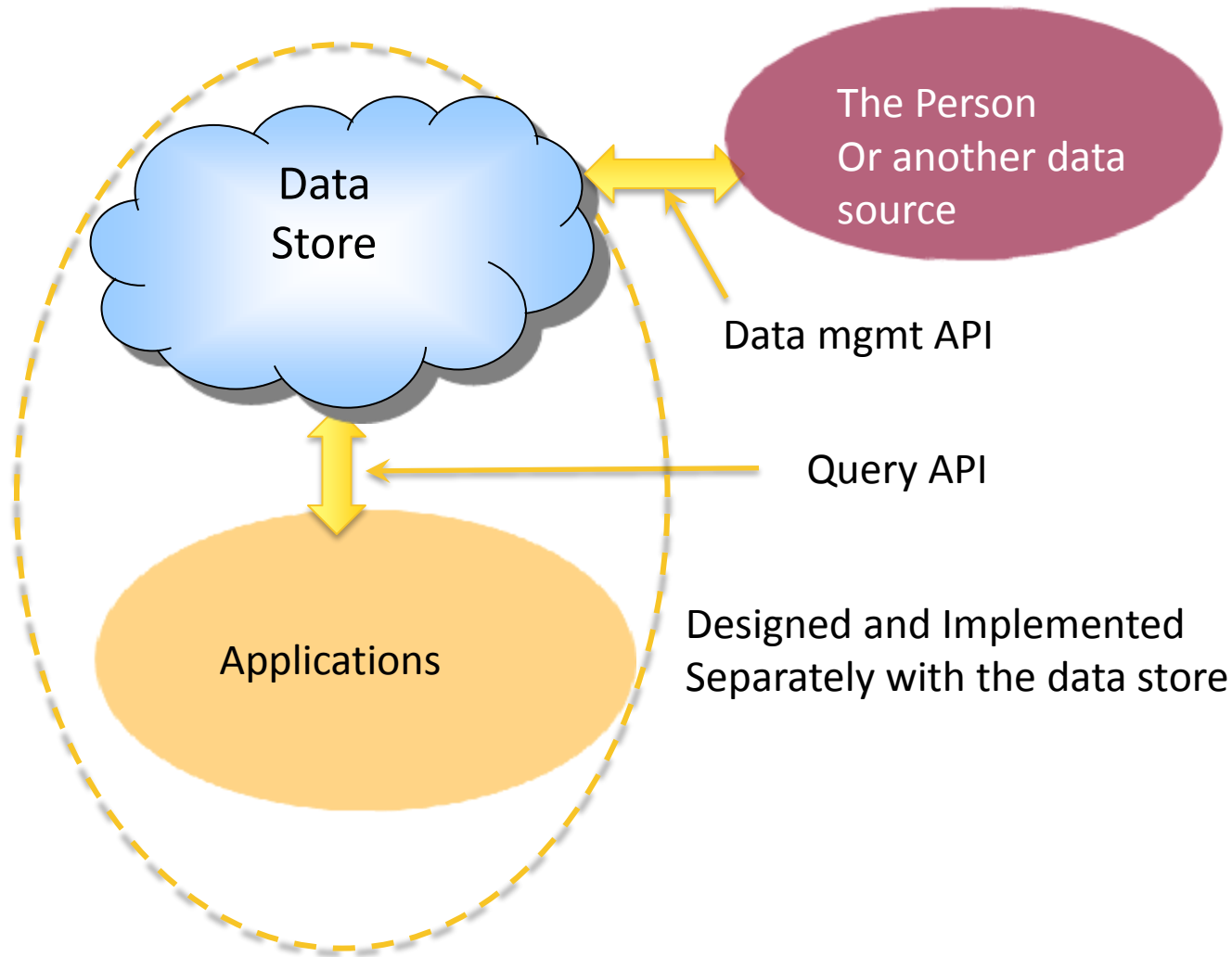
Now let's get to
the hard part -
implementation



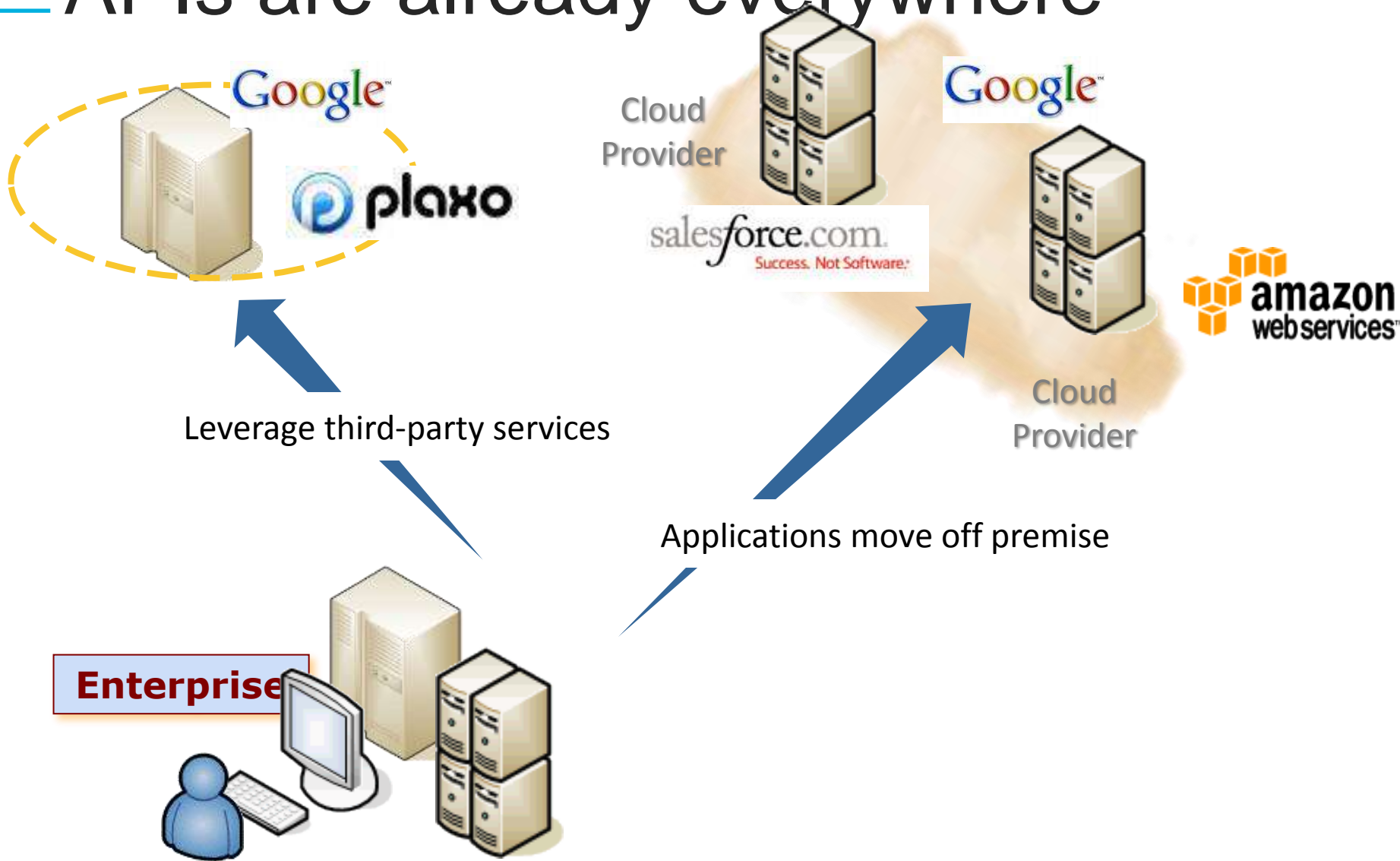
If we have a set of data stores



For each data store



APIs are already everywhere



— Going back to an earlier example

- ▶ A guy walks into a bar
- ▶ Camera takes a picture of his face sends to an “age” service

- ▶  “is this person older than 18?”

- ▶ The camera identifies itself as a bar in a particular geo and queries an “age” cloud, which holds age information of individuals
- ▶ The cloud authenticates the camera, matches the picture with stored identity information, does a “>” query, and sends the answer back
- ▶ The camera destroys the picture
- ▶ No other info is disclosed or processed

Here is our
request to the
research
community



— Many questions need to be answered

- ▶ Where are the appropriate layers of data abstractions?
- ▶ What do the APIs look like?
- ▶ How do you specify the sharing policies?
- ▶ How do you rationalize this data economy?
- ▶ How do you characterize the risk of the data?

— But the result can be transformational

- ▶ Better privacy
- ▶ More targeted information for marketer
- ▶ More transparency for consumers

Resolution 5000 x 3750 px
Free JPG file download
www.psdgraphics.com



Questions?

Alvin Tan
Alvin_tan@mcafee.com

Chenxi Wang
chenxi_wang@mcafee.com

<http://www.mcafee.com/common/privacy/english/index.htm>

