

APPLIED INTELLIGENCE: Using information that isn't there

Michael Schrenk
Las Vegas, Nevada

DEF CON XXIII

@mgschrenk



APPLIED INTELLIGENCE: Using information that isn't there



The image shows a video player interface. On the left, there is a small video thumbnail of a man with a mustache and glasses speaking at a podium. The main area of the player is a dark screen with white text. At the top, it says 'DEFCON XXI'. Below that, the title of the presentation is displayed: 'How my Botnet Purchased Millions of Dollars in Cars' followed by '- and -' and 'Defeated the Russian Hackers'. In the bottom left corner of the video area, there is a stylized logo for 'defcon 21' with various icons. At the bottom of the video player, there is a progress bar showing '0:05 / 26:52' and several control icons (play, volume, settings, full screen).

DEFCON XXI

How my Botnet Purchased
Millions of Dollars in Cars
- and -
Defeated the Russian Hackers

0:05 / 26:52

Defcon 21 - How my Botnet Purchased Millions of Dollars in Cars and Defeated the Russian Hackers

APPLIED INTELLIGENCE:

Using information that isn't there

IN ADDITION TO OTHER EXAMPLES

Retail business
my girlfriend & I own

How we CREATE and
APPLY intelligence



APPLIED INTELLIGENCE: Using information that isn't there

IN ADDITION TO OTHER EXAMPLES

Retail business
my girlfriend & I own

How we CREATE and
APPLY intelligence





APPLIED INTELLIGENCE:

Using information that isn't there

You'll hear how we use competitive intelligence to:

- 1.) Conduct intelligence campaigns on
 - a. Our competitors
 - b. Our sales channels
- 2.) Know exactly what inventory to buy
- 3.) Manipulate markets



APPLIED INTELLIGENCE:

Using information that isn't there

You'll hear how we use competitive intelligence to:

- 1.) Conduct intelligence campaigns on
 - a. Our competitors
 - b. Our sales channels
- 2.) Know exactly what inventory to buy
- 3.) Manipulate markets



APPLIED INTELLIGENCE:

Using information that isn't there

You'll hear how we use competitive intelligence to:

- 1.) Conduct intelligence campaigns on
 - a. Our competitors
 - b. Our sales channels
- 2.) Know exactly what inventory to buy
- 3.) Manipulate markets



APPLIED INTELLIGENCE:

Using information that isn't there

You'll hear how we use competitive intelligence to:

- 1.) Conduct intelligence campaigns on
 - a. Our competitors
 - b. Our sales channels
- 2.) Know exactly what inventory to buy
- 3.) Manipulate markets



APPLIED INTELLIGENCE:

Using information that isn't there

You'll hear how we use competitive intelligence to:

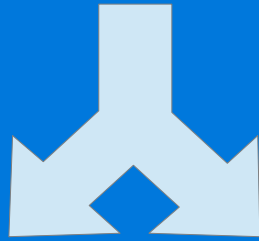
- 1.) Conduct intelligence campaigns on
 - a. Our competitors
 - b. Our sales channels
- 2.) Know exactly what inventory to buy
- 3.) ~~Manipulate markets~~

Protect Our Investment

APPLIED INTELLIGENCE:

Using information that isn't there

INTELLIGENCE



BUSINESS

COMPETITIVE

APPLIED INTELLIGENCE:

Using information that isn't there

INTELLIGENCE



BUSINESS

- What's happening within your business?
- Internal data
- Focus on efficiency
 - a.) knowing operations
 - b.) knowing resources

COMPETITIVE

- What's happening outside of your business?
- External data
- Focus on competitiveness
 - a.) knowing competitors
 - b.) knowing markets

APPLIED INTELLIGENCE:

Using information that isn't there

INTELLIGENCE



BUSINESS

- What's happening within your business?
- Internal data
- Focus on efficiency
 - a.) knowing operations
 - b.) knowing resources

COMPETITIVE

- What's happening outside of your business?
- External data
- Focus on competitiveness
 - a.) knowing competitors
 - b.) knowing markets

APPLIED INTELLIGENCE:

Using information that isn't there

INTELLIGENCE



BUSINESS

- What's happening within your business?
- Internal data
- Focus on efficiency
 - a.) knowing operations
 - b.) knowing resources

COMPETITIVE

- What's happening outside of your business?
- External data
- Focus on competitiveness
 - a.) knowing competitors
 - b.) knowing markets

APPLIED INTELLIGENCE: Using information that isn't there



Like 1.1k

[Search](#) | [Videos](#) | [Blog](#) | [Contacts](#)

[Login](#) | [Register](#) | [Register as Visitor](#)

[ABOUT SCIP](#) | [MEMBERSHIP](#) | [CHAPTERS](#) | [EDUCATION](#) | [VENDORS](#) | [ADVISORIES](#) | [EVENTS](#) | [PUBLICATIONS](#) | [PHILANTHROPY](#) | [NEWSROOM](#) | [JOBS](#)

SCIP UNIVERSITY

EDUCATION | CERTIFICATION | TRAINING ON-DEMAND



STRATEGY, MARKET & COMPETITIVE INTELLIGENCE

Established in 1986, SCIP is a global nonprofit membership organization for everyone involved in creating and managing business knowledge. Its mission is to enhance the success of its members through leadership, education, advocacy, and networking. Specifically, SCIP provides education and networking opportunities for business professionals working in the rapidly growing fields of strategy and competitive intelligence. Today SCIP has chapters as well as alliance partnerships with independent affiliate organizations around the world.

Director's Corner

WELCOME

Welcome Message from our

02 27 09

MONTHS DAYS HOURS
until the 20th Anniversary
SCIP European Summit

3 - 5 November 2015
Madrid, Spain





APPLIED INTELLIGENCE:

Using information that isn't there

Applied Intelligence = Actionable Intelligence



APPLIED INTELLIGENCE: **Using information that isn't there**

MUCH INTELLIGENCE IS USELESS

- 1.) If it won't change what you're doing it isn't useful**
- 2.) Organizations tend to over collect**
 - a.) Higher cost**
 - b.) Increased exposure**
- 3.) Intel is collected for obligatory reasons**



APPLIED INTELLIGENCE: **Using information that isn't there**

MUCH INTELLIGENCE IS USELESS

- 1.) If it won't change what you're doing it isn't useful
- 2.) Organizations tend to over collect
 - a.) Higher cost
 - b.) Increased exposure
- 3.) Intel is collected for obligatory reasons



APPLIED INTELLIGENCE: **Using information that isn't there**

MUCH INTELLIGENCE IS USELESS

- 1.) If it won't change what you're doing it isn't useful
- 2.) Organizations tend to over collect
 - a.) Higher cost
 - b.) Increased exposure
- 3.) Intel is collected for obligatory reasons

APPLIED INTELLIGENCE: Using information that isn't there



Michael Schrenk @mgschrenk · 28m

Still looking for a printable mobile-friendly #DEFCON schedule?

schrenk.com/defcon_23_print...

*there are no promises of accuracy and none as a convenience.
No rights are claimed or implied. Comments? mike@schrenk.com
Last cache Jul 24, 2015 11:42:57AM (US Pacific)*

THURSDAY					
	TRACK 1	TRACK 2	TRACK 3	TRACK 4	DEFCON 101
10:00	Empty Room	Empty Room	Empty Room	Hardware and Trust Security: Explain it like I'm 5 - Yeddy Shou & Nick Anderson	Introduction to DEF and the Wireless Village DefCon's 4 attractions
11:00	Empty Room	Empty Room	Empty Room	Backlog Web Apps - Great White	Backers Hiring Backers - How to Do Things Better - Yotam Kupch & Irit Shalom
12:00	Empty Room	Empty Room	Empty Room	Seeing through the Fog - Jack Fazel	DEF CON 101: The Panel - Panel
13:00	Empty Room	Empty Room	Empty Room	Alleg and Day are Really Confused - David Morris	DEF CON 101: The Panel - Panel
14:00	Empty Room	Empty Room	Empty Room	Backer in the Wilds - Dr. Phil Feltrin	Beyond the Scan: The Value Proposition of Vulnerability Assessment - Jason Smith
15:00	Empty Room	Empty Room	Empty Room	Forensic Artifacts From a Free the Cash Attack - Gerard Lippert	Responsible Incident: Covert Eggs Against Subverted Technology - Latencies, Especially - Rubikay - Jodl
16:00	Empty Room	Empty Room	Empty Room	Rocky, Wrong Number / Mysteries Of The Phone System - Past and Present: "Unregistered" & "Misde" Over	Overle E' Collins: Exposing Me-Fi: Infiltration Risks and Mitigation Techniques - Peter Hefpiger, Johann Schuster & Gerald O'Leary
				Backdooring Bit - [Small text]	Dark side of the ELF - [Small text]

APPLIED INTELLIGENCE: Using information that isn't there



Michael Schrenk @mgschrenk · 28m

Still looking for a printable mobile-friendly #DEFCON schedule?
schrenk.com/defcon_23_print...

*there are no promises of accuracy and none as a convenience.
 No rights are claimed or implied. Comments? mike@schrenk.com
 Last cache Jul 24, 2015 11:42:57AM (US Pacific)*

THURSDAY					
	TRACK 1	TRACK 2	TRACK 3	TRACK 4	DEFCON 101
10:00	Empty Room	Empty Room	Empty Room	Hardware and Trust Security: Explain it like I'm 5 - Yoddy Hood & Nick Adleyson	Introduction to DEF and the Wireless Village - JeffHorta & @stuck4less
11:00	Empty Room	Empty Room	Empty Room	Backing Web Apps - Great White	Hackers Hiring Hackers - How to Do Things Better - Yotiankaph & Iristh@ms
12:00	Empty Room	Empty Room	Empty Room	Seeing through the Fog - Jack Fazel	DEF CON 101: The Panel - Panel
13:00	Empty Room	Empty Room	Empty Room	Alice and Bob and Really Cool - David Garcia	DEF CON 101: The Panel - Panel
14:00	Empty Room	Empty Room	Empty Room	Hacker in the Wild - Dr. M. Palstra	Beyond the Scan: The Value Proposition of Vulnerability Assessment - Jason Ross
15:00	Empty Room	Empty Room	Empty Room	Impacts From a Pure Cash Attack - David Lippert	Responsible Incident: Covert Says Against Subverted Technology - Latentia, Especially Tubiley - Jodl
16:00	Empty Room	Empty Room	Empty Room	Keylog, Strong Passwords, Passwords Of The Past - @j00n and Frazee - @j00n & @frazee	David E. Gollins: Exposing Wi-Fi - Penetration Tests and Mitigation Techniques - Peter Hoffigler, Joshua Orlowski, David G. Lippert

Collected:
 Access time
 IP Addresses
 Frequency accessed (cookie)
 User Agent
 Referrer

APPLIED INTELLIGENCE: Using information that isn't there



Applied Intelligence: Using Information That's Not There
Michael Schrenk

APPLIED INTELLIGENCE: Using information that isn't there

 **Applied Intelligence: Using Information That's Not There**
Michael Schrenk

TIME	TRACK 01	TRACK 02	TRACK 03	TRACK 04	DEFCON 101
01:00 PM					<input checked="" type="checkbox"/>
02:00 PM		<input checked="" type="checkbox"/>			
03:00 PM	<input checked="" type="checkbox"/>				
04:00 PM				<input checked="" type="checkbox"/>	
05:00 PM			<input checked="" type="checkbox"/>		

APPLIED INTELLIGENCE: Using information that isn't there

 **Applied Intelligence: Using Information That's Not There**
Michael Schrenk

TIME	TRACK 01	TRACK 02	TRACK 03	TRACK 04	DEFCON 101
01:00 PM					<input checked="" type="checkbox"/>
02:00 PM		<input checked="" type="checkbox"/>			
03:00 PM	<input checked="" type="checkbox"/>				
04:00 PM				<input checked="" type="checkbox"/>	
05:00 PM			<input checked="" type="checkbox"/>		

Information (in aggregate) could predict talk popularity and affect planning



APPLIED INTELLIGENCE:

Using information that isn't there

Information
that
isn't there = Meta data

APPLIED INTELLIGENCE:

Using information that isn't there

Meta data

The public did not know much about meta data before the Snowden disclosures



Edward Snowden

APPLIED INTELLIGENCE:

Using information that isn't there

**"As you know, this is just meta data.
There is no content involved."**

Dianne Feinstein

June 6, 2013 Intelligence Comm. Briefing



APPLIED INTELLIGENCE:

Using information that isn't there

“Nobody is listening to your telephone calls. That’s not what this program is about...”

*They’re not looking at names and they’re not looking at content, but **sifting through this so-called meta data...**”*

*Barack Obama, on NSA Surveillance
June 7, 2014*



APPLIED INTELLIGENCE:

Using information that isn't there

```
$sql = "  
    sift(*)  
    from  
    phone_records  
    where  
    person = 'suspect'  
";
```

APPLIED INTELLIGENCE:

Using information that isn't there

"We kill people based on meta data."

*Former NSA Boss, Michael Hayden
May 11, 2014 Johns Hopkins University*





APPLIED INTELLIGENCE:

Using information that isn't there

Meta data:

- 1.) Describes other data
- 2.) Provides context for information
- 3.) It often *doesn't exist* & it needs to be created.



APPLIED INTELLIGENCE:

Using information that isn't there

Meta data:

- 1.) Describes other data
- 2.) Provides context for information
- 3.) It often *doesn't exist* & it needs to be created.



APPLIED INTELLIGENCE:

Using information that isn't there

Meta data:

- 1.) Describes other data
- 2.) Provides context for information
- 3.) It often *doesn't exist* & it needs to be created.



APPLIED INTELLIGENCE:

Using information that isn't there

Meta data types

- 1.) Parametric *must be collected / created*
- 2.) Embedded *user created*



APPLIED INTELLIGENCE:

Using information that isn't there

Meta data types

- 1.) Parametric *must be collected / created*
- 2.) Embedded *user created*

APPLIED INTELLIGENCE:

Using information that isn't there

Meta Data: Embedded



XIF Geo-Codes
leaked that
Russian soldiers
were in Ukraine

APPLIED INTELLIGENCE:

Using information that isn't there

Meta Data: Embedded

The Tony Blair memo
Justification for invading Iraq



The screenshot shows the top navigation bar of The Guardian website. It includes a 'sign in' button with a user icon, a search bar with a magnifying glass icon, and links for 'jobs' and 'US edition'. The main logo 'theguardian' is prominently displayed. Below the logo is a breadcrumb trail: 'home > world > middle east africa australia cities development UK europ ≡ all'. The main content area features the sub-header 'UK news' and the headline 'Downing St admits blunder on Iraq dossier'. A sub-headline below reads 'Plagiarism row casts shadow over No 10's case against Saddam'.

sign in search jobs US edition ▾

theguardian

home > world > middle east africa australia cities development UK europ ≡ all

UK news

Downing St admits blunder on Iraq dossier

Plagiarism row casts shadow over No 10's case against Saddam

APPLIED INTELLIGENCE:

Using information that isn't there

Meta Data: Embedded

```
1 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd
2 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd
3 : cic22 : C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd
4 : JPratt : C:\TEMP\Iraq - security.doc
5 : JPratt : A:\Iraq - security.doc
6 : ablackshaw : C:\ABlackshaw\Iraq - security.doc
7 : ablackshaw : C:\ABlackshaw\A;Iraq - security.doc
8 : ablackshaw : A:\Iraq - security.doc
9 : MKhan : C:\TEMP\Iraq - security.doc
10 : MKhan : C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc
```

APPLIED INTELLIGENCE: Using information that isn't there

Meta Data: Embedded



Google CEO, Eric Schmidt, leaked the existence of new project “Google Drive”



APPLIED INTELLIGENCE:

Using information that isn't there

**How the NSA uses
Parametric Meta Data**



APPLIED INTELLIGENCE:

Using information that isn't there

Phone meta data collected by the NSA*:

- 1.) Phone numbers of parties**
- 2.) The time the call was placed**
- 3.) The duration of the call**
- 4.) Who initiated the call**



APPLIED INTELLIGENCE:

Using information that isn't there

Phone meta data collected by the NSA*:

- 1.) Phone numbers of parties
- 2.) The time the call was placed
- 3.) The duration of the call
- 4.) Who initiated the call



APPLIED INTELLIGENCE:

Using information that isn't there

Phone meta data collected by the NSA*:

- 1.) Phone numbers of parties
- 2.) The time the call was placed
- 3.) The duration of the call
- 4.) Who initiated the call

*https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf



APPLIED INTELLIGENCE:

Using information that isn't there

Phone meta data collected by the NSA*:

- 1.) Phone numbers of parties**
- 2.) The time the call was placed**
- 3.) The duration of the call**
- 4.) Who initiated the call**

APPLIED INTELLIGENCE:

Using information that isn't there

Phone meta data collected by the NSA*:

The NSA does what

- 1.) Phone number of the parties
- 2.) The time of the call placed
- 3.) The duration of the call
- 4.) Who initiated the call



APPLIED INTELLIGENCE:

Using information that isn't there

With this meta data:

- 1.) Caller relationships are established**
- 2.) These relationships can be profiled**
- 3.) Anomalies and outliers are identified**
- 4.) “Burner phones” are identified**
- 5.) Phone patterns can be tied to other events**



APPLIED INTELLIGENCE:

Using information that isn't there

With this meta data:

- 1.) Caller relationships are established
- 2.) These relationships can be profiled
- 3.) Anomalies and outliers are identified
- 4.) “Burner phones” are identified
- 5.) Phone patterns can be tied to other events



APPLIED INTELLIGENCE:

Using information that isn't there

With this meta data:

- 1.) Caller relationships are established
- 2.) These relationships can be profiled
- 3.) Anomalies and outliers are identified
- 4.) “Burner phones” are identified
- 5.) Phone patterns can be tied to other events



APPLIED INTELLIGENCE:

Using information that isn't there

With this meta data:

- 1.) Caller relationships are established
- 2.) These relationships can be profiled
- 3.) Anomalies and outliers are identified
- 4.) “Burner phones” are identified
- 5.) Phone patterns can be tied to other events



APPLIED INTELLIGENCE:

Using information that isn't there

With this meta data:

- 1.) Caller relationships are established
- 2.) These relationships can be profiled
- 3.) Anomalies and outliers are identified
- 4.) “Burner phones” are identified
- 5.) Phone patterns can be tied to other events



APPLIED INTELLIGENCE:

Using information that isn't there

**The phone meta data is richer
than the actual phone
conversations**

But the meta data needs to be created.



APPLIED INTELLIGENCE: Using information that isn't there

Practical
competitive
intelligence

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

A reviewal of day-to-day operations, to see what intelligence an advisory can collect.



APPLIED INTELLIGENCE:

Using information that isn't there

EMPLOYMENT
POSTINGS

OPSEC

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

EMPLOYMENT
POSTINGS

SOCIAL
MEDIA

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

**EMPLOYMENT
POSTINGS**

**SOCIAL
MEDIA**

**ORDER
FULFILLMENT**

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

**EMPLOYMENT
POSTINGS**

**SOCIAL
MEDIA**

**ORDER
FULFILLMENT**

**ONLINE
STORE**

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

EMPLOYMENT
POSTINGS

SOCIAL
MEDIA

ORDER
FULFILLMENT

ONLINE
STORE

PROCUREMENT

APPLIED INTELLIGENCE:

Using information that isn't there

OPSEC

REGULATORY

EMPLOYMENT
POSTINGS

SOCIAL
MEDIA

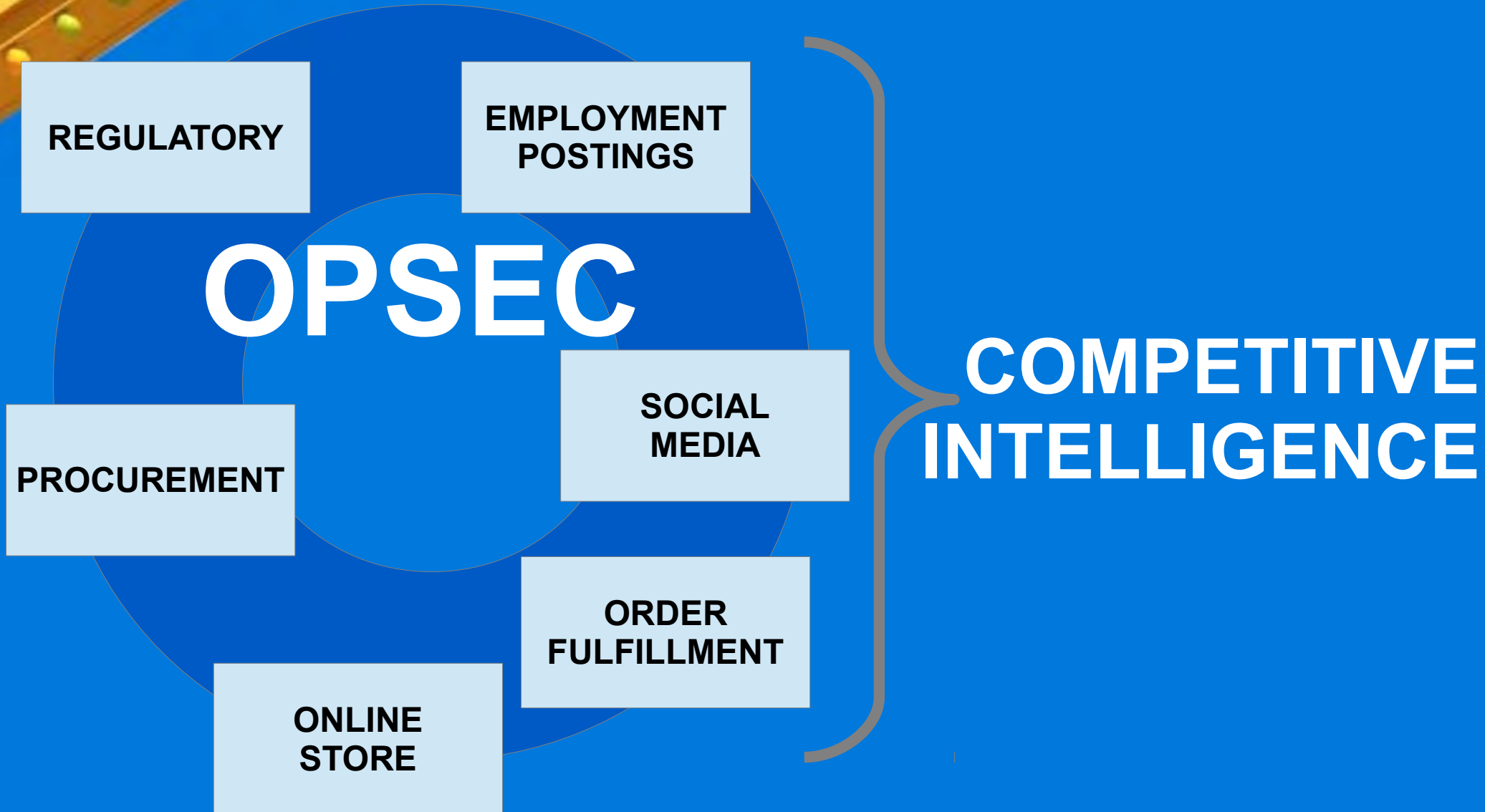
ORDER
FULFILLMENT

ONLINE
STORE

PROCUREMENT

APPLIED INTELLIGENCE:

Using information that isn't there



APPLIED INTELLIGENCE:

Using information that isn't there

Sequential numbers are a major
privacy threat



APPLIED INTELLIGENCE:

Using information that isn't there

Sequential Numbers

Sequential Numbers are everywhere
Vehicle Identification Numbers
Social Security Numbers
Ticket Numbers



In most cases, what's needed are **unique** numbers, not **sequential** numbers.

Often caused by **exposing DB table indexes**



APPLIED INTELLIGENCE:

Using information that isn't there

**To show the power of
sequential numbers...**

**I'm going to tell you how the Social Security
Administration nearly exposed an entire
generation to identity fraud.**



APPLIED INTELLIGENCE:

Using information that isn't there

SSN coding 1935 through 1972

XXX – XX – XXXX

AREA

GROUP

SERIAL

Area	State, Territory or US possession (<i>range</i>)
Group	Used for administration purposes
Serial	Sequential (<i>with a few exceptions</i>)

APPLIED INTELLIGENCE: Using information that isn't there

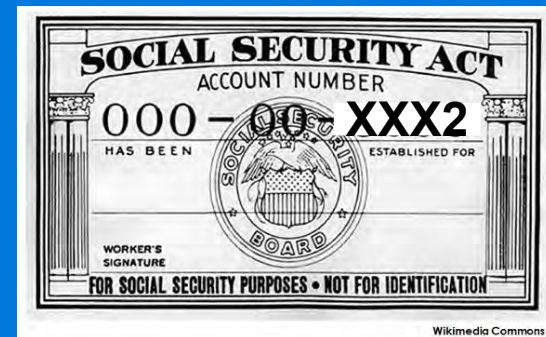
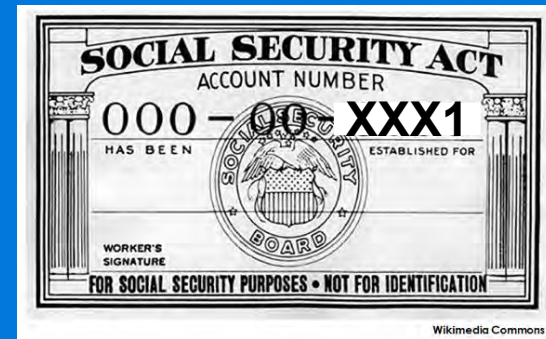
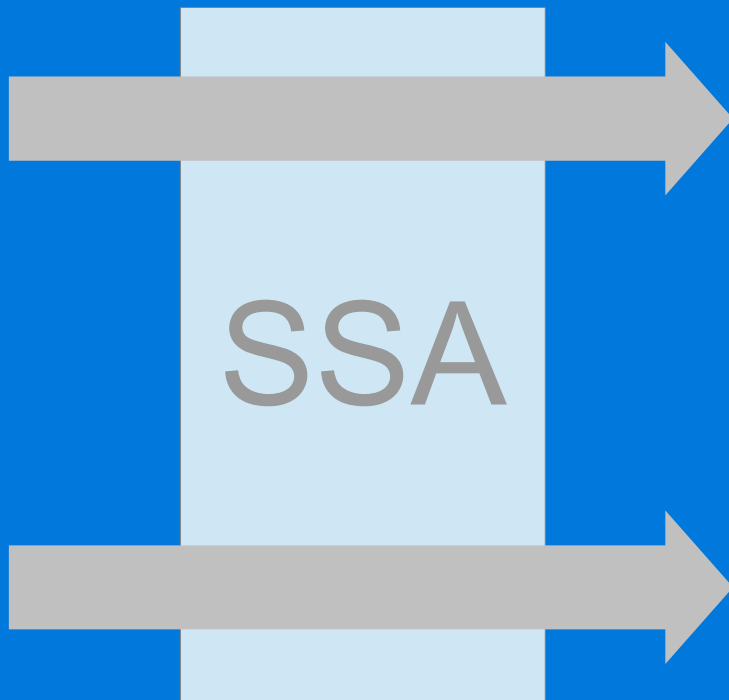
Applying for cards, 1932 - 1972



Age 14



Age 15



These people have sequential SSNs

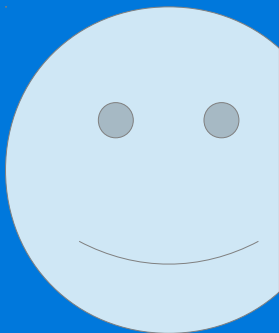
APPLIED INTELLIGENCE:

Using information that isn't there

Applying for cards, 1932 - 1972



Age 14



Age 15

This process changed In 1972

The last for digits
were no longer
sequential



These people have sequential SSNs

APPLIED INTELLIGENCE:

Using information that isn't there

**Tax
Reform
Act of
1986**



Social Security

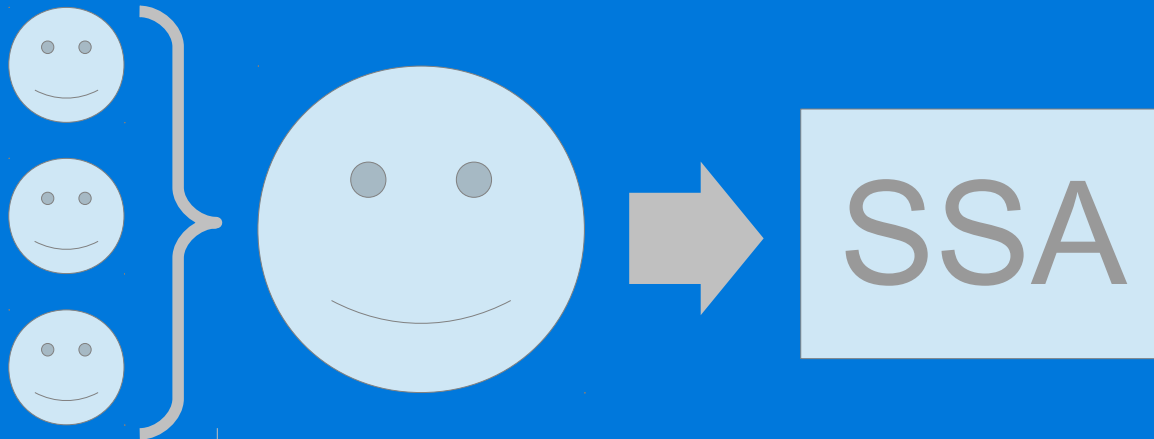
Social Security
Numbers For
Children

Parents needed SSNs for all dependents

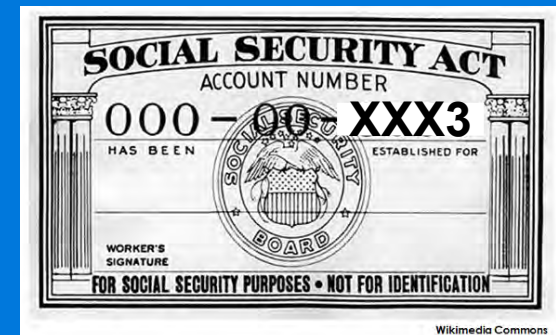
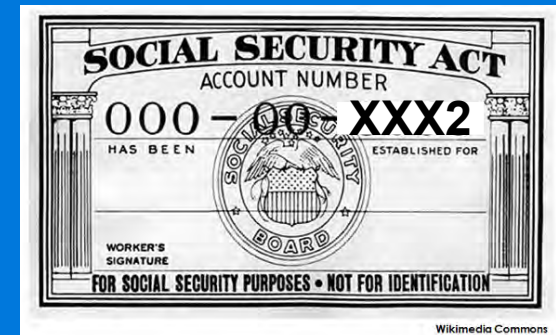
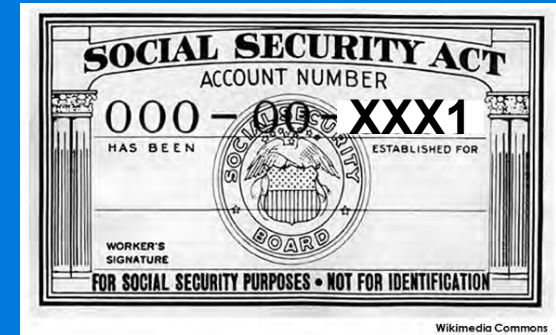
APPLIED INTELLIGENCE:

Using information that isn't there

If sequential numbers were still used in the '80s



Needs SSNs for children to declare as dependents



These children would have sequential Social Security Numbers



APPLIED INTELLIGENCE:

Using information that isn't there

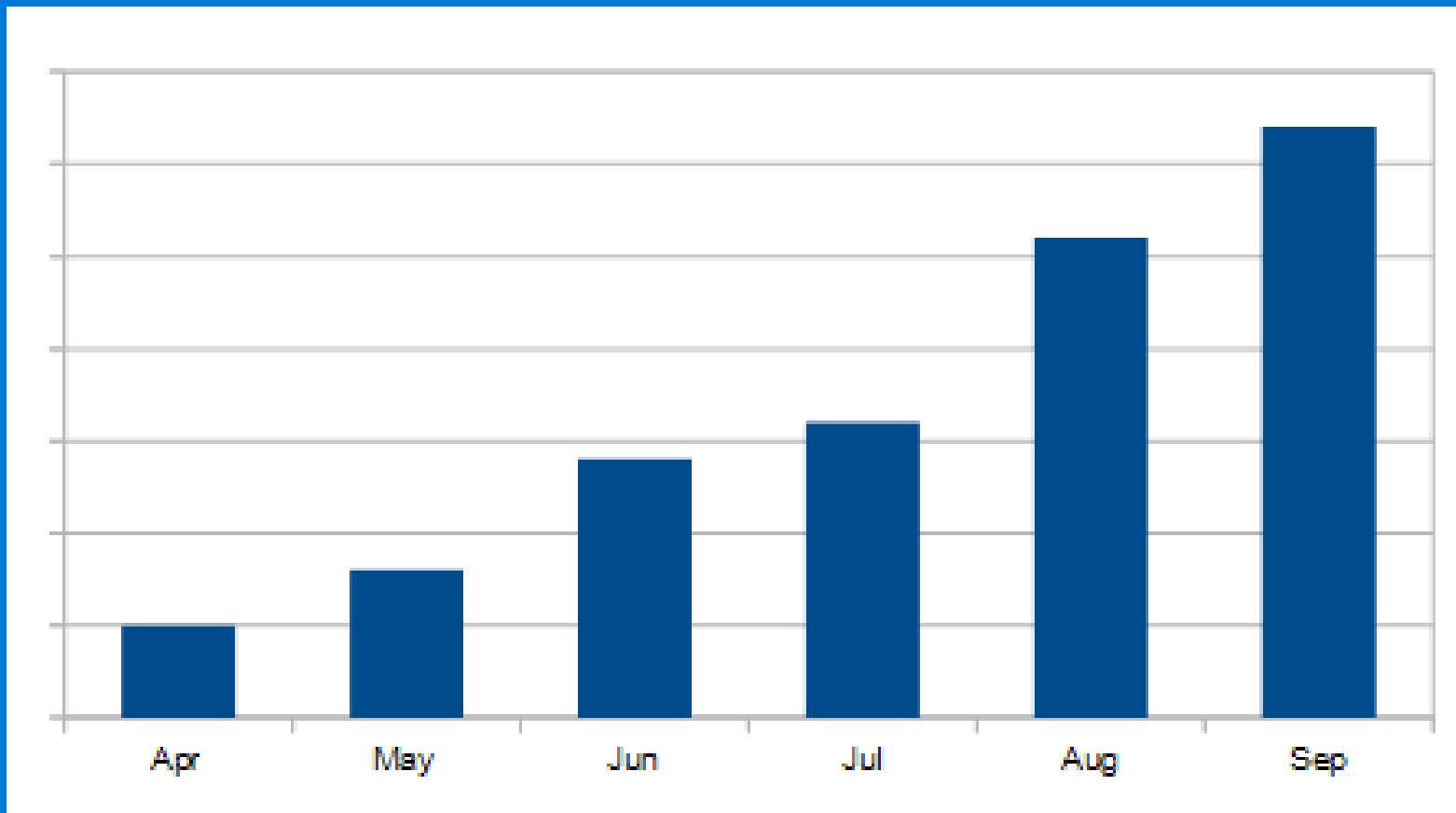
**How we use
sequential numbers
in our business**

**Did we start our business at
the height of a bubble?**

APPLIED INTELLIGENCE:

Using information that isn't there

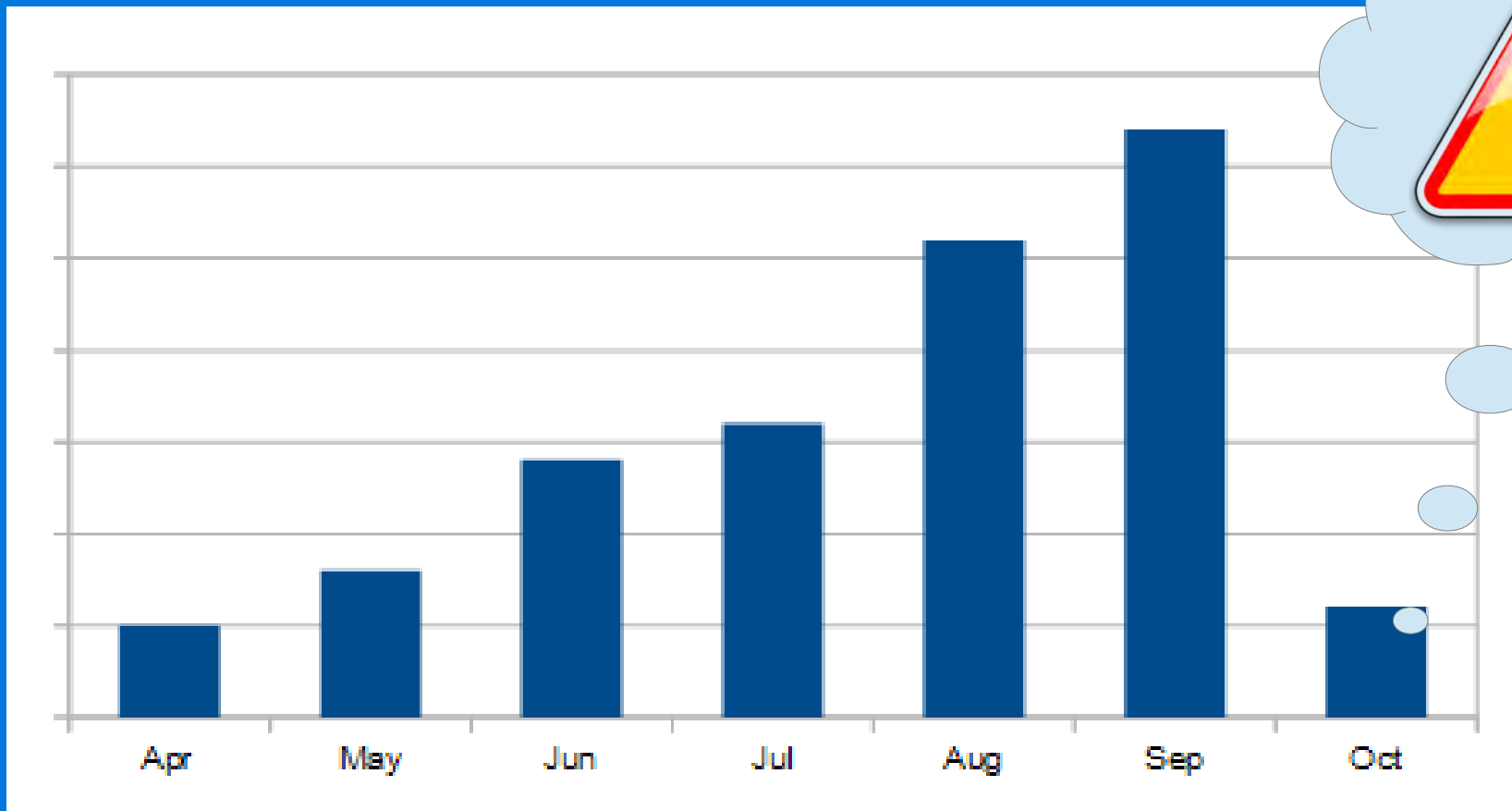
Channel Sales



APPLIED INTELLIGENCE:

Using information that isn't there

Bubble or just a bad month?





APPLIED INTELLIGENCE: **Using information that isn't there**

Bubble or just a bad month?

- 1.) We noticed that order numbers were incremental**
- 2.) We found two orders, placed closely together, had SEQUENTIAL order numbers**



APPLIED INTELLIGENCE:

Using information that isn't there

Bubble or just a bad month?

- 1.) We noticed that order numbers were incremental
- 2.) We found two orders, placed closely together, had SEQUENTIAL order numbers

APPLIED INTELLIGENCE:

Using information that isn't there

Last Order# Oct:	763736
Last Order# Sep:	<u>-757225</u>
Qty Oct orders (est)	6511

- 1.) Our average order was \$12.48
- 2.) Determined our orders were typical

Average Sale:	\$12.48
Estimated July orders	<u>x 6511</u>
Gross Channel Sales	\$81,257.28

APPLIED INTELLIGENCE:

Using information that isn't there

Last Order# Oct:	763736
Last Order# Sep:	<u>-757225</u>
Qty Oct orders (est)	6511

- 1.) Our average order was \$12.48
- 2.) Determined our orders were typical

Average Sale:	\$12.48
Estimated July orders	<u>x 6511</u>
Gross Channel Sales	\$81,257.28

APPLIED INTELLIGENCE:

Using information that isn't there

Last Order# Oct:	763736
Last Order# Sep:	<u>-757225</u>
Qty Oct orders (est)	6511

- 1.) Our average order was \$12.48
- 2.) Determined our orders were typical

Average Sale:	\$12.48
Estimated July orders	<u>x 6511</u>
Gross Channel Sales	\$81,257.28

APPLIED INTELLIGENCE:

Using information that isn't there

Total Channel Sales

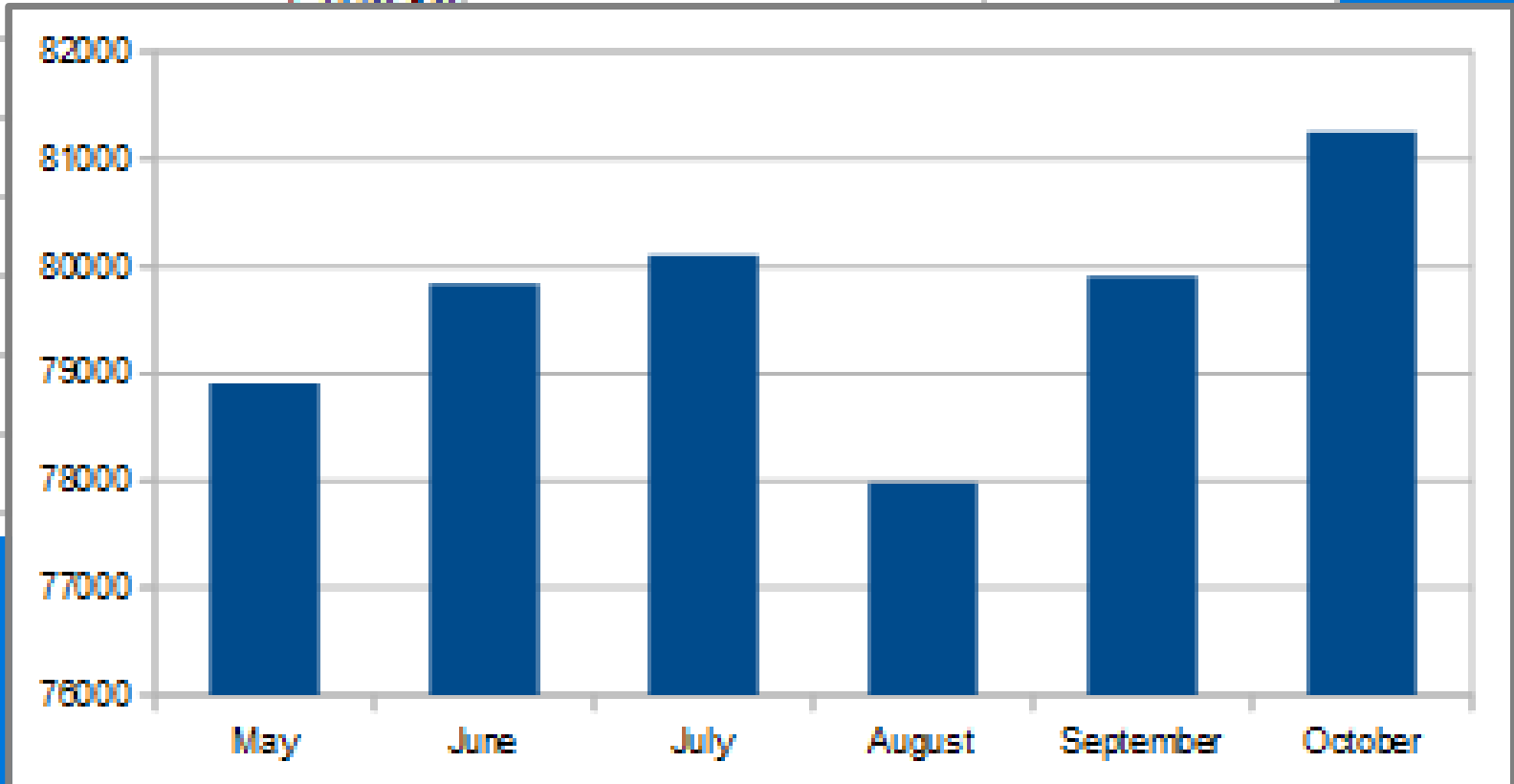
MONTH	LAST ORDER #	QTY ORDERS	GROSS \$
April	725434	-	-
May	731757	6323	\$78,911.04
June	738154	6397	\$79,834.56
July	744573	6419	\$80,109.12
August	750822	6249	\$77,987.52
September	757225	6403	\$79,909.44
October	763736	6511	\$81,257.28

APPLIED INTELLIGENCE:

Using information that isn't there

Total Channel Sales

MONTH	LAST ORDER #	QTY ORDERS	GROSS \$
April	776434		
May			
June			
July			
August			
September			
October			





APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

- 1.) What else do we know?
- 2.) Channel commission is ~ 20%
- 3.) They keep \$1.25 of the postage they collect.



APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

- 1.) What else do we know?**
- 2.) Channel commission is ~ 20%**
- 3.) They keep \$1.25 of the postage they collect.**



APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

- 1.) What else do we know?
- 2.) Channel commission is ~ 20%
- 3.) They keep \$1.25 of the postage they collect.

APPLIED INTELLIGENCE:

Using information that isn't there

Here is how much the website earns in commissions each month

MONTH	LAST ORDER #	QTY ORDERS	GROSS \$	COMMISSION
April	725434	-	-	-
May	731757	6323	\$78,911.04	\$15,782.21
June	738154	6397	\$79,834.56	\$15,966.91
July	744573	6419	\$80,109.12	\$16,021.82
August	750822	6249	\$77,987.52	\$15,597.50
September	757225	6403	\$79,909.44	\$15,981.89
October	763736	6511	\$81,257.28	\$16,251.46



APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

- 1.) What else do we know?
- 2.) Channel commission is ~ 20%
- 3.) They keep \$1.25 of the postage they collect.

APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

MONTH	LAST ORDER #	QTY ORDERS	GROSS \$	COMMISSION	POSTAGE	PROFIT
April	725434	-	-	-	-	-
May	731757	6323	\$78,911.04	\$15,782.21	\$7,903.75	\$23,685.96
June	738154	6397	\$79,834.56	\$15,966.91	\$7,996.25	\$23,963.16
July	744573	6419	\$80,109.12	\$16,021.82	\$8,023.75	\$24,045.57
August	750822	6249	\$77,987.52	\$15,597.50	\$7,811.25	\$23,408.75
September	757225	6403	\$79,909.44	\$15,981.89	\$8,003.75	\$23,985.64
October	763736	6511	\$81,257.28	\$16,251.46	\$8,138.75	\$24,390.21

Avg Monthly profit: \$23913.22

Est Annual profit: \$286958.58

APPLIED INTELLIGENCE:

Using information that isn't there

What else can we learn?

This is probably information
They'd prefer not to share

MONTH	LAST ORDER #	QTY ORDERS	GROSS \$	COMMISSION	POSTAGE	PROFIT
April	725034	6397	\$79,834.58	\$15,986.91	\$7,996.25	\$23,963.16
May	731571	6419	\$80,409.42	\$16,021.89	\$8,033.75	\$24,045.57
June	738154	6403	\$79,909.44	\$15,981.89	\$8,003.75	\$23,985.64
July	744573	6511	\$81,257.28	\$16,251.46	\$8,138.75	\$24,390.21
August	751002					
September	751225					
October	763736					

Avg Monthly profit: \$23913.22
Est Annual profit: \$286958.58

APPLIED INTELLIGENCE:

Using information that isn't there

How do we buy inventory

There are websites
where we buy

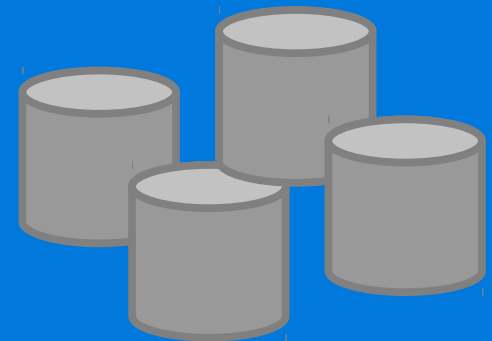


APPLIED INTELLIGENCE:

Using information that isn't there

How do we buy inventory

There are websites where we buy



We sell on multiple websites, but only one is “a true market”



APPLIED INTELLIGENCE:

Using information that isn't there

How do we buy inventory

We look for items
And prices here



APPLIED INTELLIGENCE:

Using information that isn't there

How do we buy inventory

We look for items
And prices here



And compare those
prices to the
market value



APPLIED INTELLIGENCE:

Using information that isn't there

How do we buy inventory

#	AVAILABLE ITEM			MARKET		ACTION
	Item	Location	Price	Price	Margin	
1.	Source_8	<i>Some item description</i>	6.74	3.14	46.59%	ignore
2.	Source_1	<i>Some item description</i>	3.22	19.48	604.97%	<u>BUY</u>
3.	Source_8	<i>Some item description</i>	2.76	5.85	211.96%	ignore
4.	Source_1	<i>Some item description</i>	3.23	5.38	166.56%	ignore
5.	Source_8	<i>Some item description</i>	8.81	1.34	15.21%	ignore
6.	Source_2	<i>Some item description</i>	1.39	12.24	880.58%	<u>BUY</u>
7.	Source_8	<i>Some item description</i>	2.25	3.38	150.22%	ignore
8.	Source_5	<i>Some item description</i>	2.50	5.43	217.20%	ignore
9.	Source_2	<i>Some item description</i>	1.36	1.59	116.91%	ignore
10.	Source_7	<i>Some item description</i>	1.33	3.56	267.67%	ignore



APPLIED INTELLIGENCE:

Using information that isn't there

There are major privacy issues for resellers that sell unique items



APPLIED INTELLIGENCE:

Using information that isn't there

There are major privacy issues for resellers that sell unique items

Truly unique items:

- Real estate**
- Vehicles**
- Original art**

Likely unique items:

- First edition books**
- Autographed items**
- Most used items**



APPLIED INTELLIGENCE:

Using information that isn't there

There are major privacy issues for resellers that sell unique items

Truly unique items:

- Real estate**
- Vehicles**
- Original art**

Likely unique items:

- First edition books**
- Autographed items**
- Most used items**

APPLIED INTELLIGENCE:

Using information that isn't there

What makes the best competitor the best?

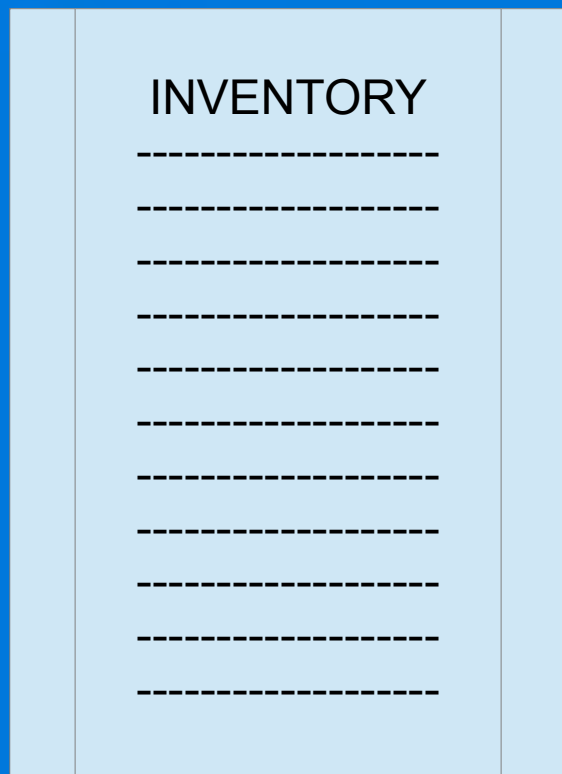
INVENTORY

Automatically collect the inventory of our top competitor

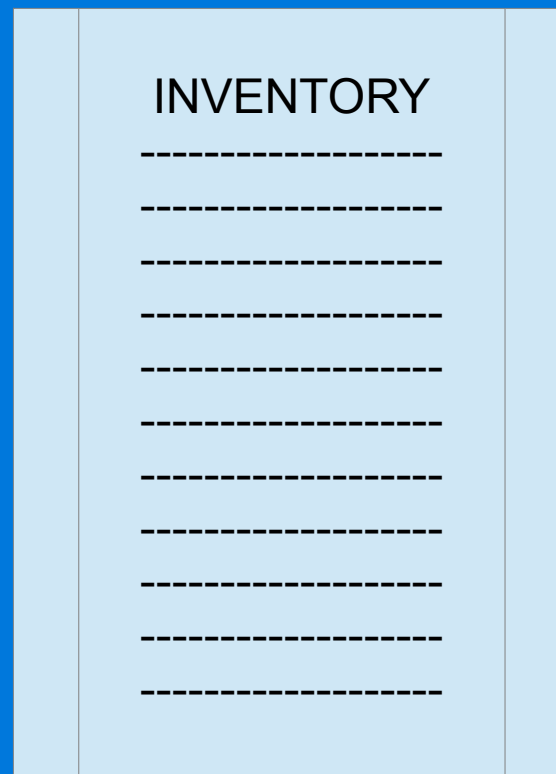
APPLIED INTELLIGENCE:

Using information that isn't there

What makes the best competitor the best?



Capture #1

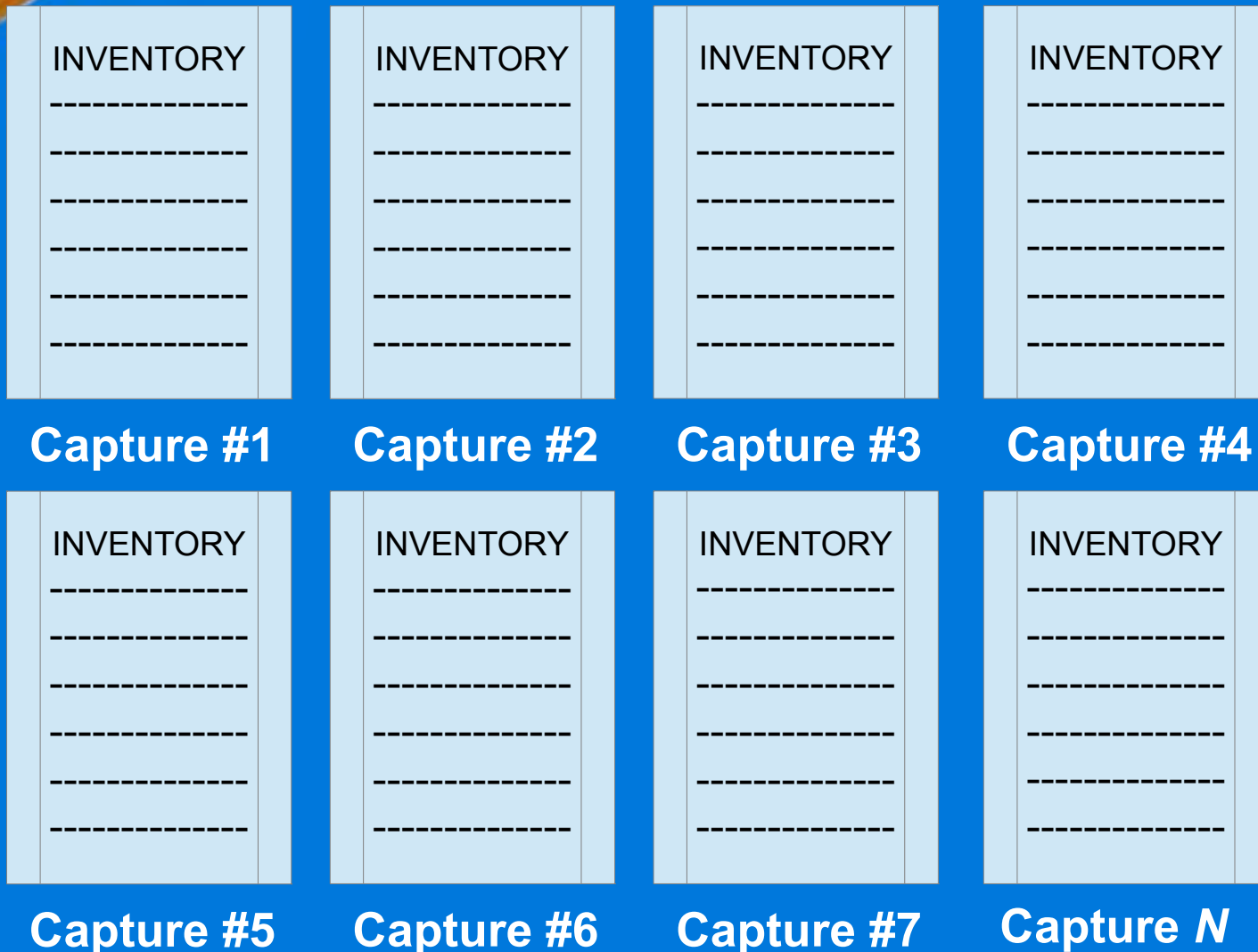


Capture #2

Meta data describing:
What sold?
How much?
What didn't sell?

APPLIED INTELLIGENCE: Using information that isn't there

What makes the best competitor the best?



Meta data describing:

What sold?
How much?
How long?

What didn't sell?

APPLIED INTELLIGENCE:

Using information that isn't there

How do we protect our investments?

ACME ITEM #1

#1	seller "A"	\$1.25
#2	seller "B"	\$1.25
#3	seller "C"	\$19.50
#4	seller "D"	\$20.05
#5	seller "E"	\$21.95

Our price

Search results for
an item we sell

APPLIED INTELLIGENCE:

Using information that isn't there

How do we protect our investments?

ACME ITEM #1

#1	seller "A"	\$1.25
#2	seller "B"	\$1.25
#3	seller "C"	\$19.50
#4	seller "D"	\$20.05
#5	seller "E"	\$21.95

Our price

Search results for
an item we sell

We immediately
buy the
under-priced items



APPLIED INTELLIGENCE:

Using information that isn't there

If you find this subject interesting...

Follow me on Twitter
[@mgschrenk](https://twitter.com/mgschrenk)

Watch defcon.org
for updated slides

[@mgschrenk](https://twitter.com/mgschrenk)

APPLIED INTELLIGENCE: Using information that isn't there

If you find this subject interesting...



The screenshot shows the top navigation bar of The Christian Science Monitor website, including the logo, 'Log In | Register', 'FREE E-mail Newsletters', and a 'Subscribe' button. Below the navigation is a green banner for 'Passcode' with the tagline 'Modern field guide to security and privacy'. The main article is titled 'Michael Schrenk on stealing data your company gives away for free' and is by Joe Uchill, dated July 30, 2015. The article text discusses a presentation at Def Con in Las Vegas. A photo of Michael Schrenk is shown at the bottom left. On the right, there are two advertisement boxes for 'Van Cleef & Arpels' featuring 'Heure d'ici & Heure d'ailleurs' in Los Angeles and 'FRENCH RIVIERA' for crafting personal fragrances.

The CHRISTIAN SCIENCE
MONITOR

Log In | Register
FREE E-mail Newsletters

Passcode | The Monitor Breakfast

World | USA | Commentary | Business | Energy / Environment | Technology | Science | Culture | Books | Take Action | Search | Subscribe

Passcode
Modern field guide to security and privacy

WORLD | PASSCODE

Michael Schrenk on stealing data your company gives away for free

In advance of his presentation at the Def Con conference in Las Vegas, Passcode spoke with Schrenk about the insider information he's paid to glean from the open Internet - and how companies can better protect themselves from having their inside plans exposed or used against them by competitors.

By Joe Uchill, Staff writer | JULY 30, 2015

Save for later



Courtesy of Michael Schrenk | View Caption

Van Cleef & Arpels

Heure d'ici & Heure d'ailleurs

LOS ANGELES

Virginia Robinson Garden:
Arguably the city's most serene address, visitable by appointment only, with a personal Friends of Robinson Gardens ambassador guide.

FRENCH RIVIERA

Crafting personal fragrances:
Create and file your own fragrance in a private atelier session with a *maitre* of Galimard, one of France's oldest *parfumeurs*.

About these ads

@mgschrenk

APPLIED INTELLIGENCE:

Using information that isn't there

If you find this subject interesting...

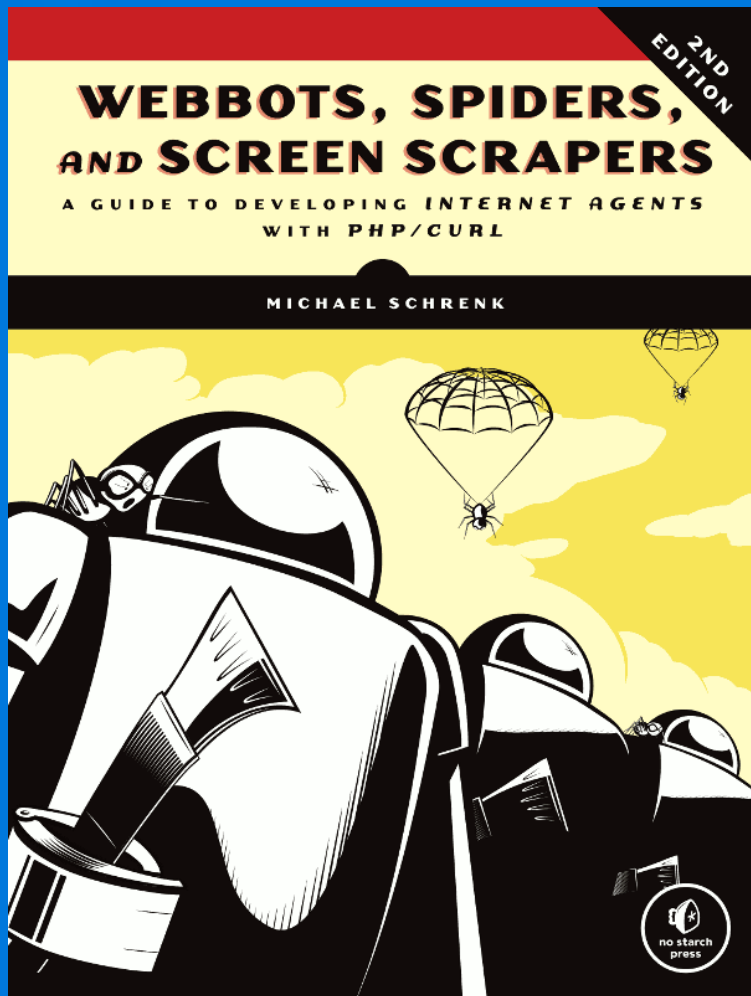


@mgschrenk

APPLIED INTELLIGENCE:

Using information that isn't there

If you find this subject interesting...



I'm doing a book signing
@ No Starch
booth in vendor
area

@mgschrenk