# The Golden Age of Surveillance

## Australian Cyber Conference 2019

**Thomas Drake**

*8 October 2019*

NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

- BEFORE -

No Such Agency

Never Say Anything

Never Share Anything

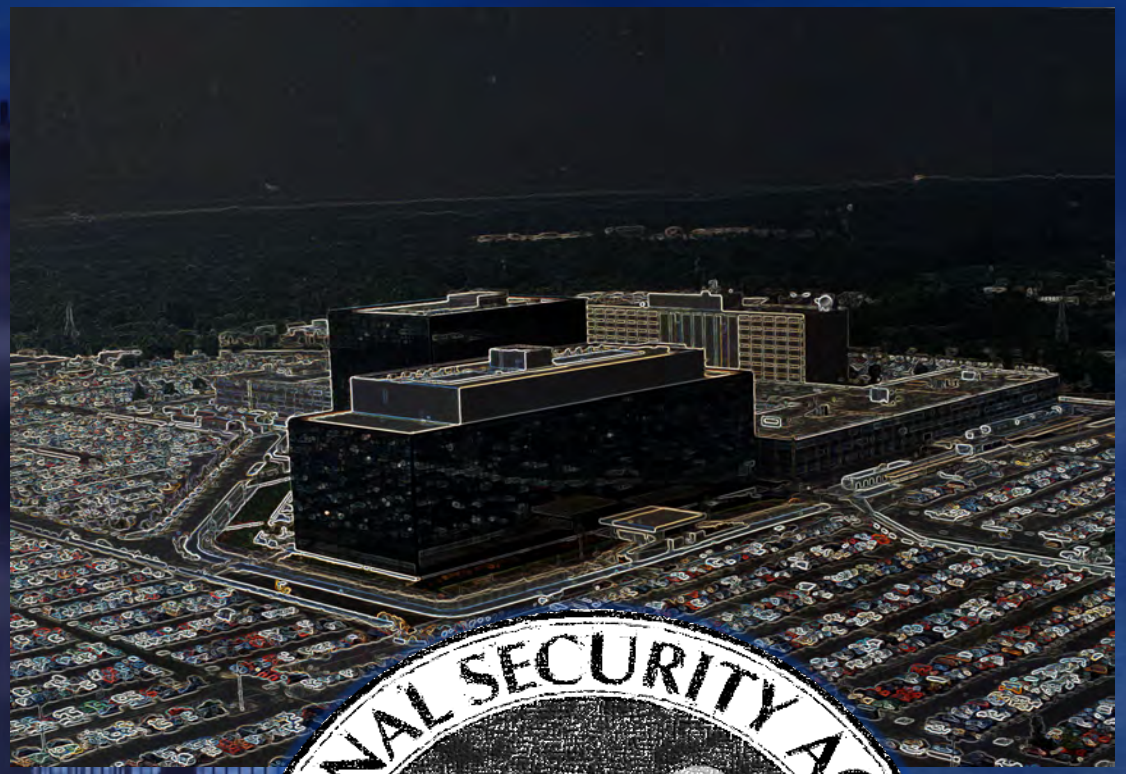
- AFTER -

No Security Anymore

No Secrets Anymore

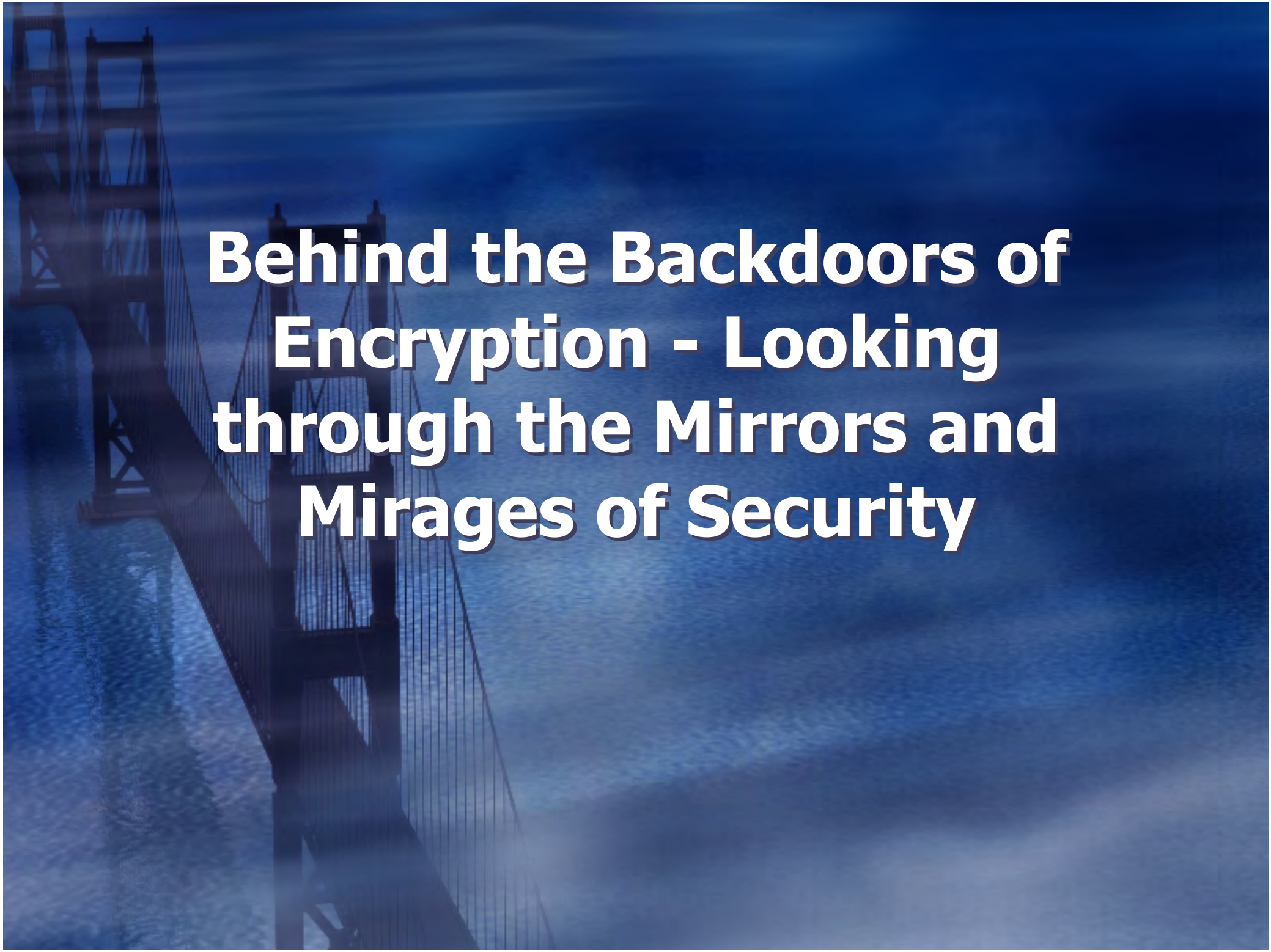
National Surveillance Agency

# Or?!

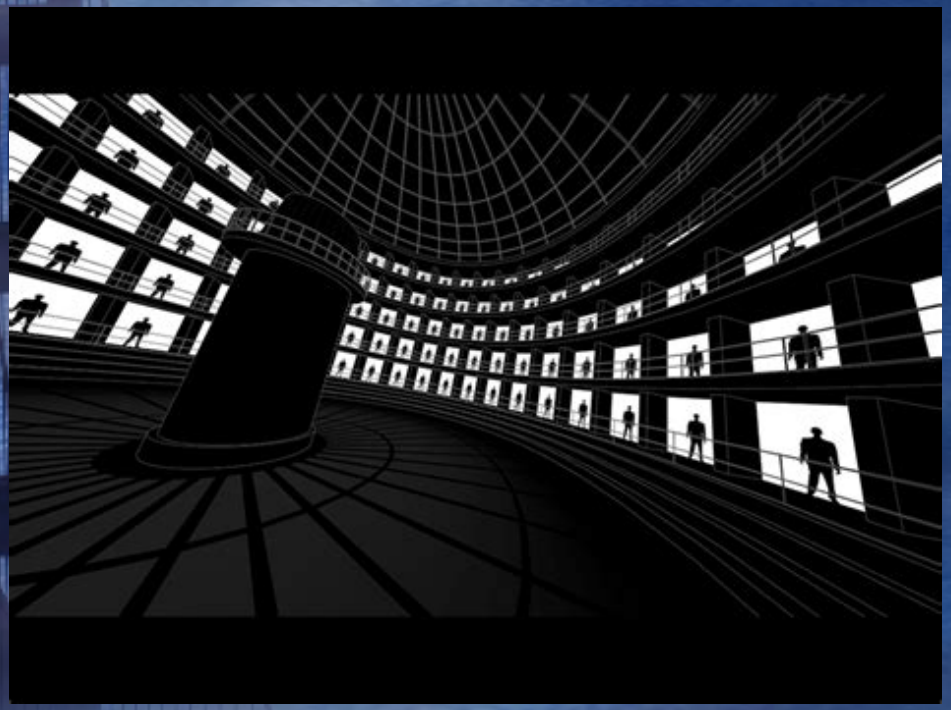


# Or?? Or?? Orwell…ian??

# The Golden Age of Computing!


Behind the Backdoors of Encryption - Looking through the Mirrors and Mirages of Security

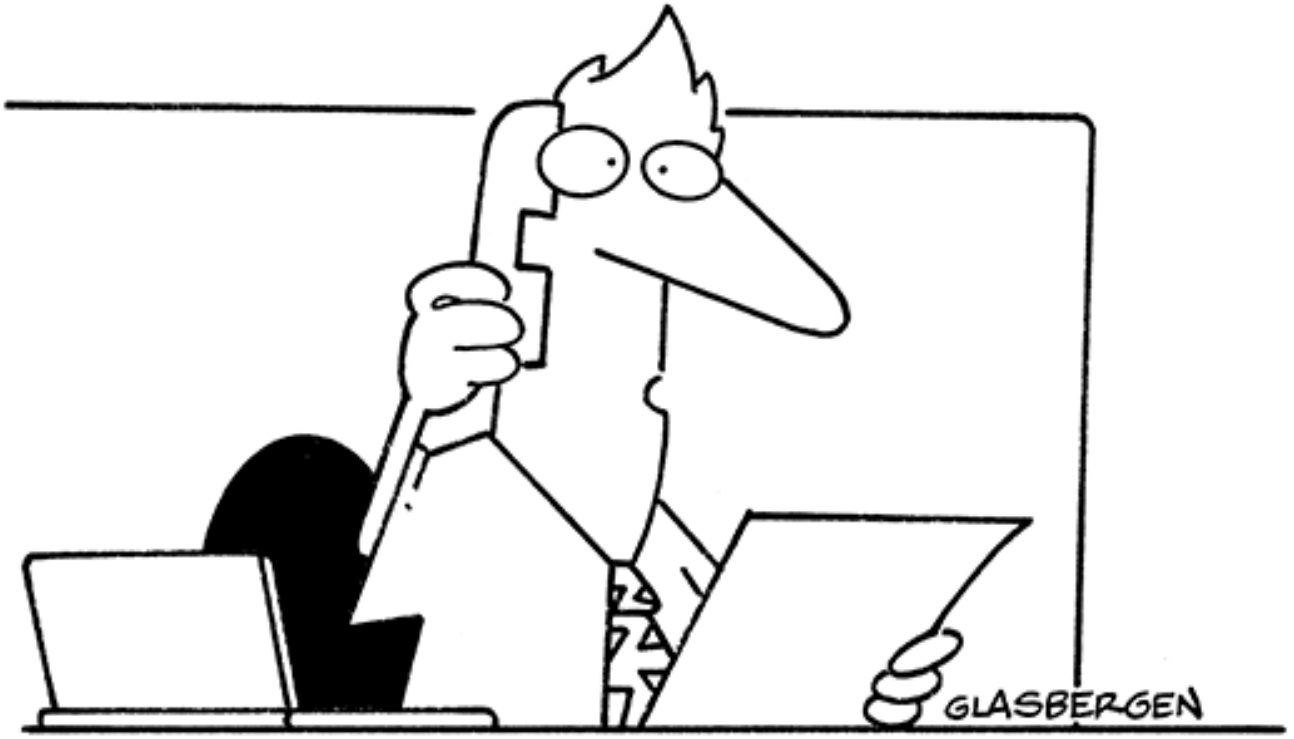
# The Panopticon
# Visibility – It's a Trap!




© Randy Glasbergen / glasbergen.com
GLASBERGEN
"The usual stuff — a new virus from the Joker, spyware from the Penguin, malicious code from Cat Woman, another phishing scheme from the Riddler."

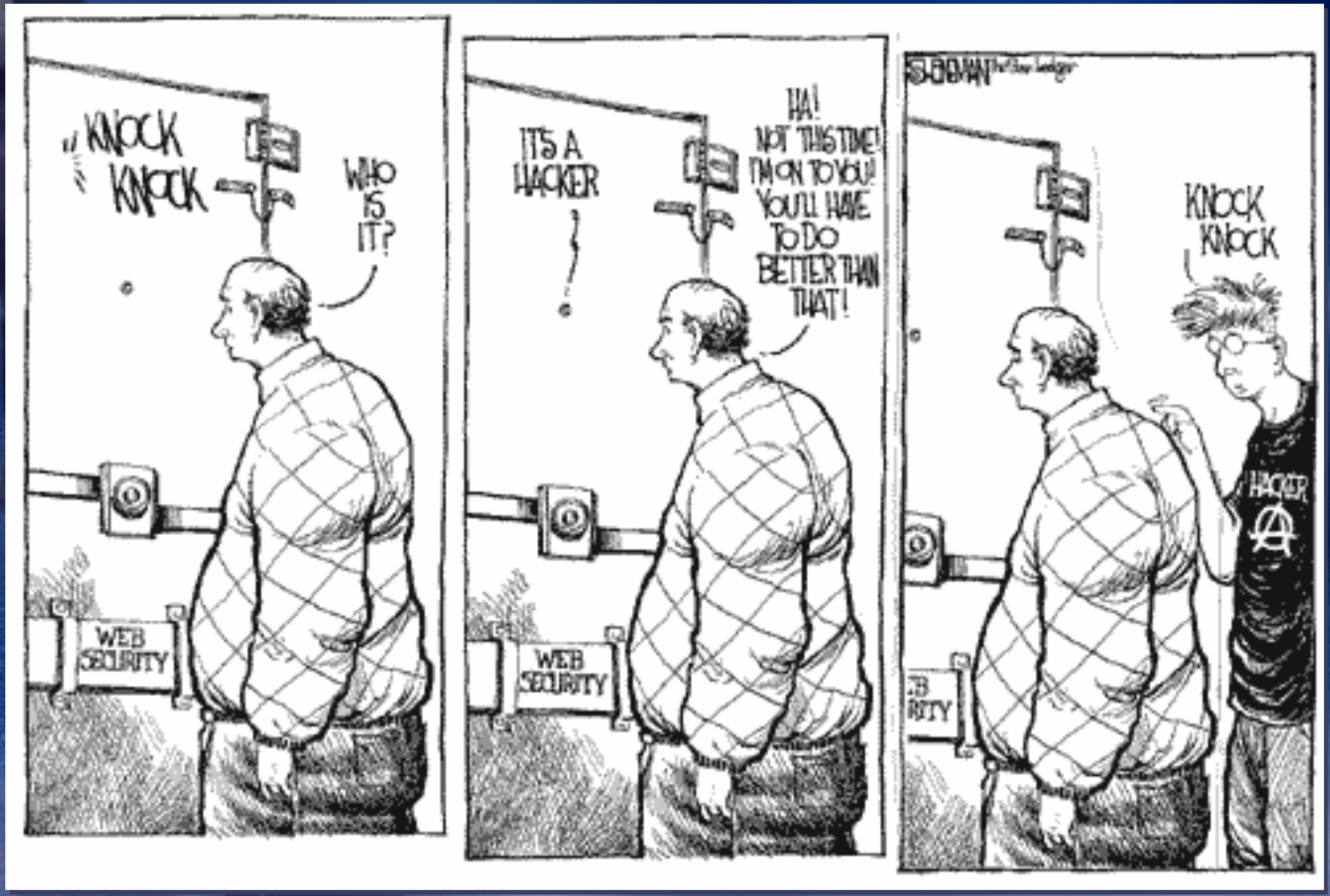

**"I used to bury my bones.
Now I upload them to the cloud."**


Security AND Privacy?!
Oxymoronic?!




**"Information security is becoming a huge problem around here. Do you still have my Captain Crunch decoder ring, Mom?"**

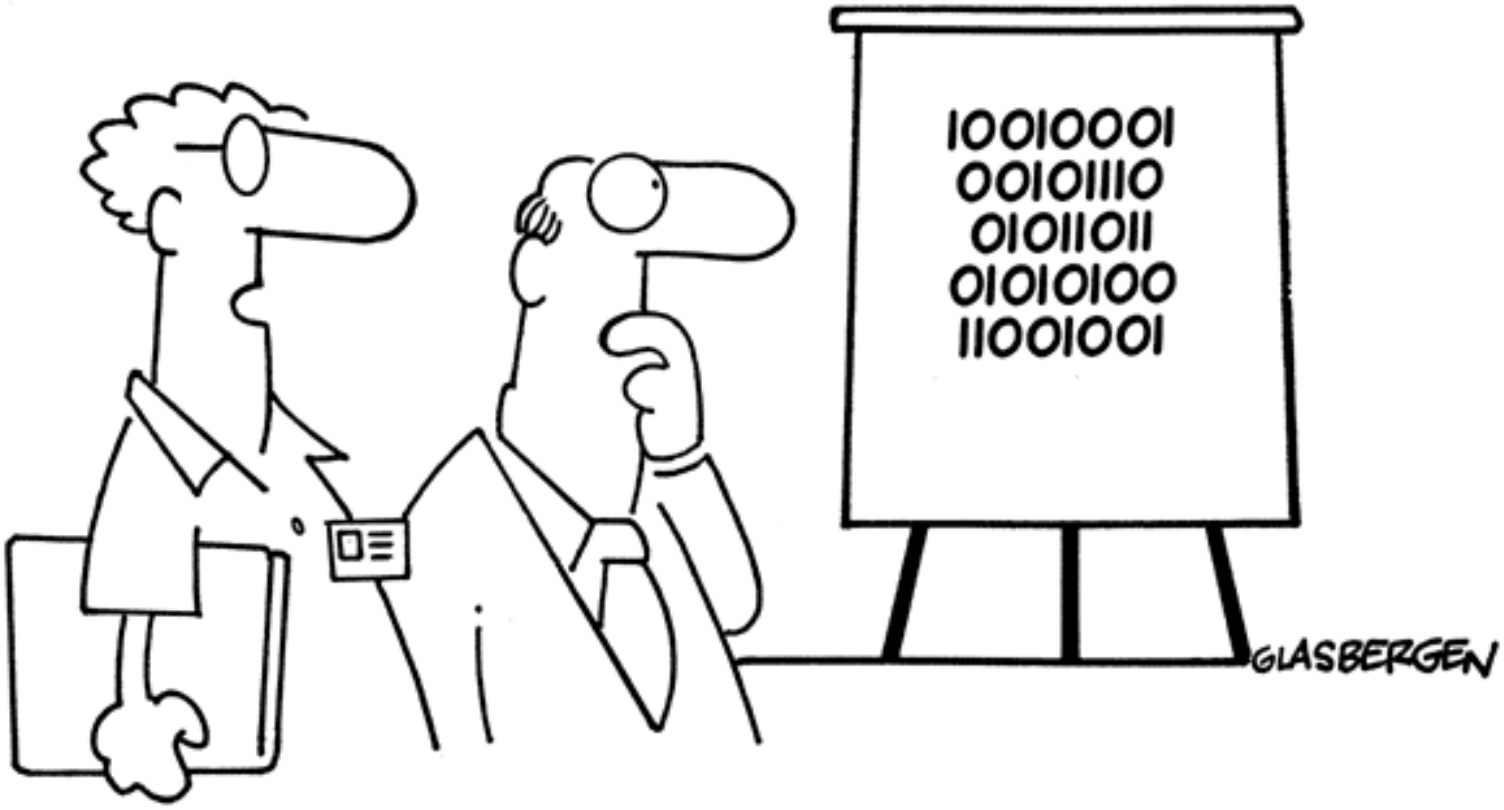
# Information Insecurity
## *Illusion and Delusion*


KNOCK KNOCK
WHO IS IT?
WEB SECURITY
IT'S A HACKER!
HA! NOT THIS TIME! I'M ON TO YOU! YOU'LL HAVE TO DO BETTER THAN THAT!
WEB SECURITY
KNOCK KNOCK
HACKER

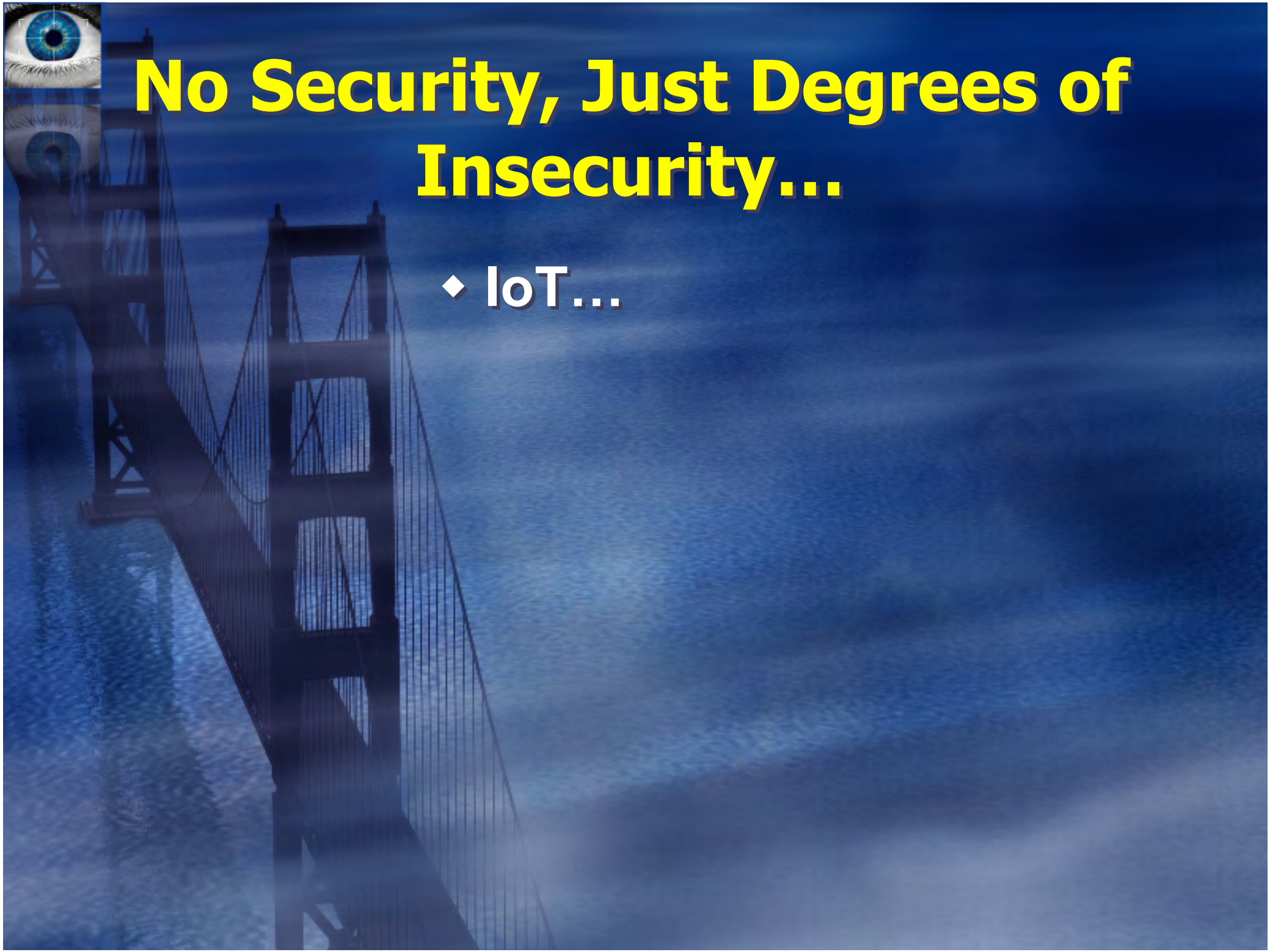
# A Personal Story
# Why a Safe is not Safe


Enjoy Security!
diplomat


I STOLE THE ENEMY'S ENCRYPTION-BREAKING SOFTWARE.
Dilbert.com @ScottAdamsSays
MY PHONE DOESN'T HAVE A HOLE FOR THIS. I THINK IT NEEDS AN ADAPTER OR SOMETHING.
4-23-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick
IS IT TIME TO ADMIT WE'RE IN OVER OUR HEADS?
WHY ARE THE HEATHENS SO GOOD AT THIS STUFF?




**"We've devised a new security encryption code. Each digit is printed upside down."**


No Security, Just Degrees of Insecurity…
IoT…

DES ruled in the land for over 20 years. Academics studied him intently. For the first time, there was something specific to look at. The modern field of cryptography was born.

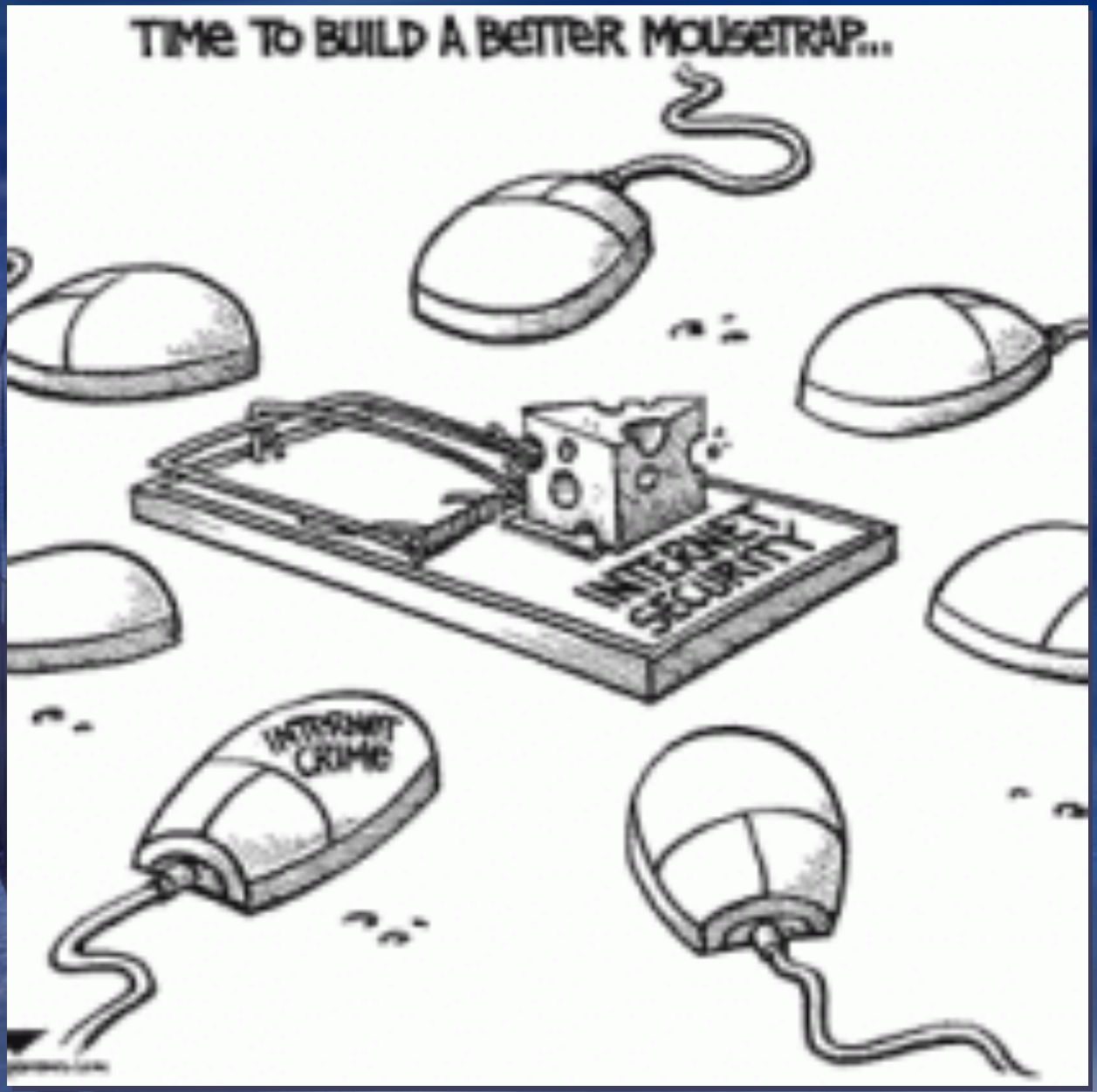
"... to the best of our knowledge, DES is free from any statistical or mathematical weakness."

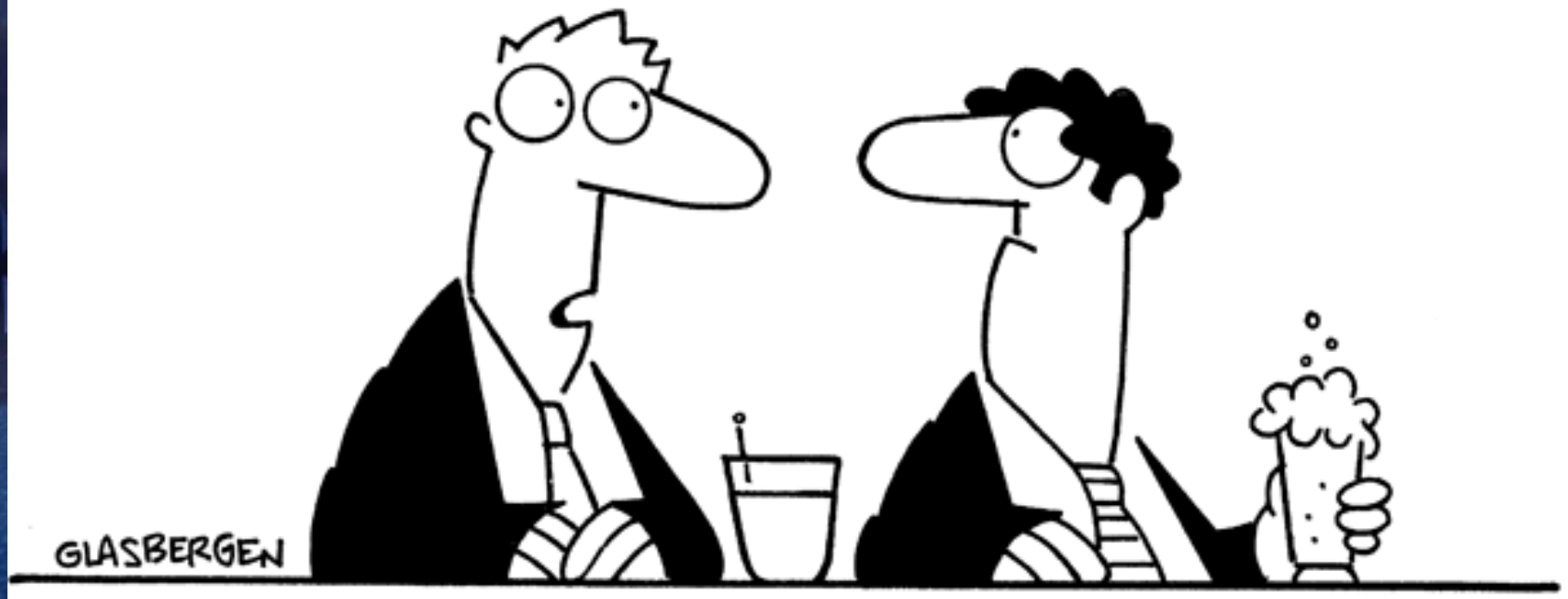
NSA

Check out that Feistel network!

Zzzz


RSA!?!


TIME TO BUILD A BETTER MOUSETRAP...
INTERNET SECURITY




**"While I was thinking outside of the box, someone changed the password and now I can't get back in!"**

# So Simple It Fits in a Tweet

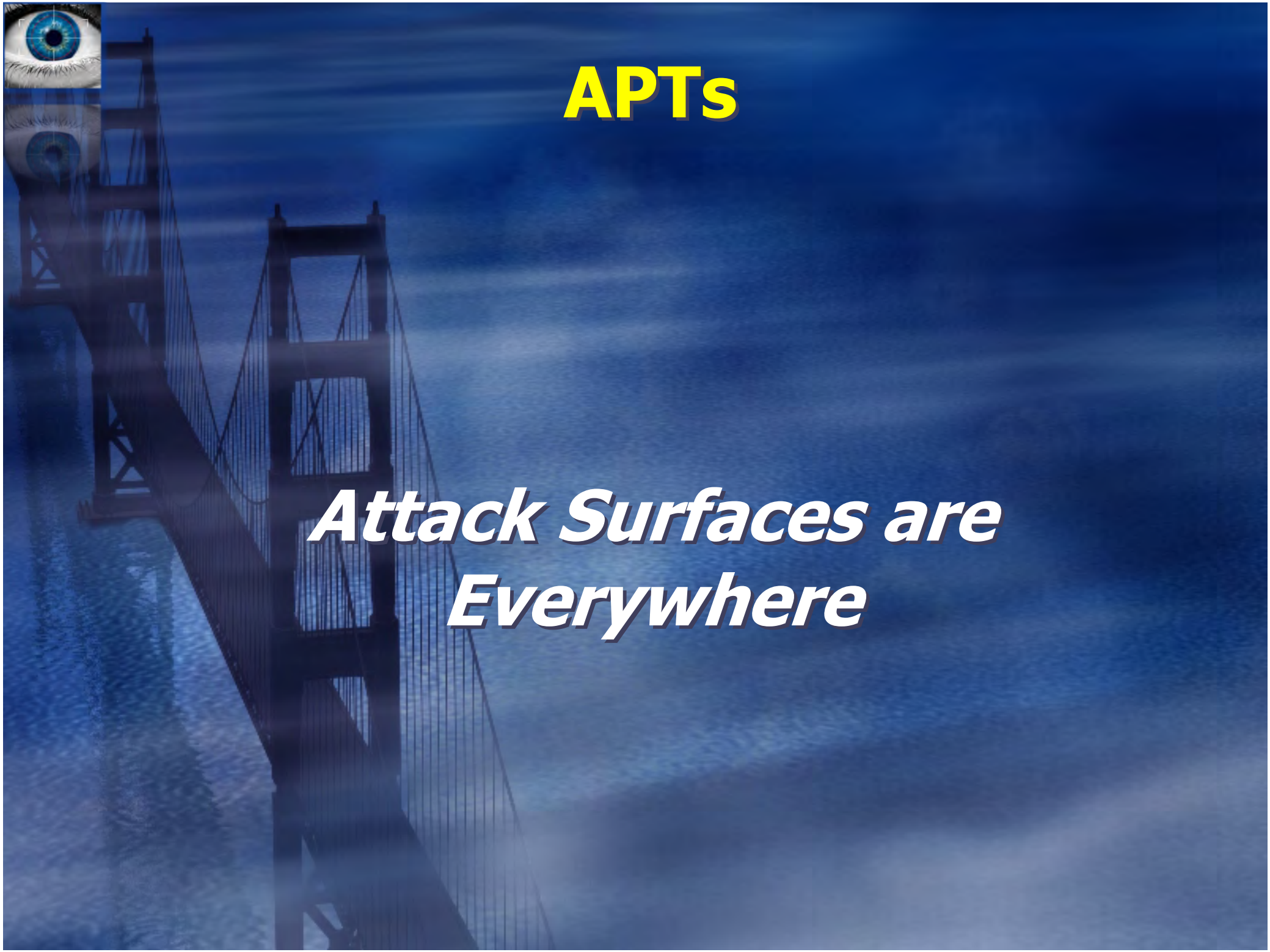
- Argentinian security researcher Ezequiel Fernandez published CVE-2018-9995, a vulnerability discovered in dozens of brands of DVR that are all based on the same white-label devices, TBK's DVR4104 and DVR4216.

- How? Just hit the URL for the embedded web-server that controls the device with this cookie header: "Cookie: uid=admin" The DVR then returns the root login and password in the clear. Some 55,000 devices with this vulnerability were indexed by the Shodan search engine.
- proof-of-concept exploit for the vulnerability, called get DVR_Credentials;
- Curl “http://{DVR_HOST_IP}:{PORT}/device.rsp?opt=user&cmd=list" -H "Cookie: uid=admin"

- https://boingboing.net/2018/05/08/morzilla.html

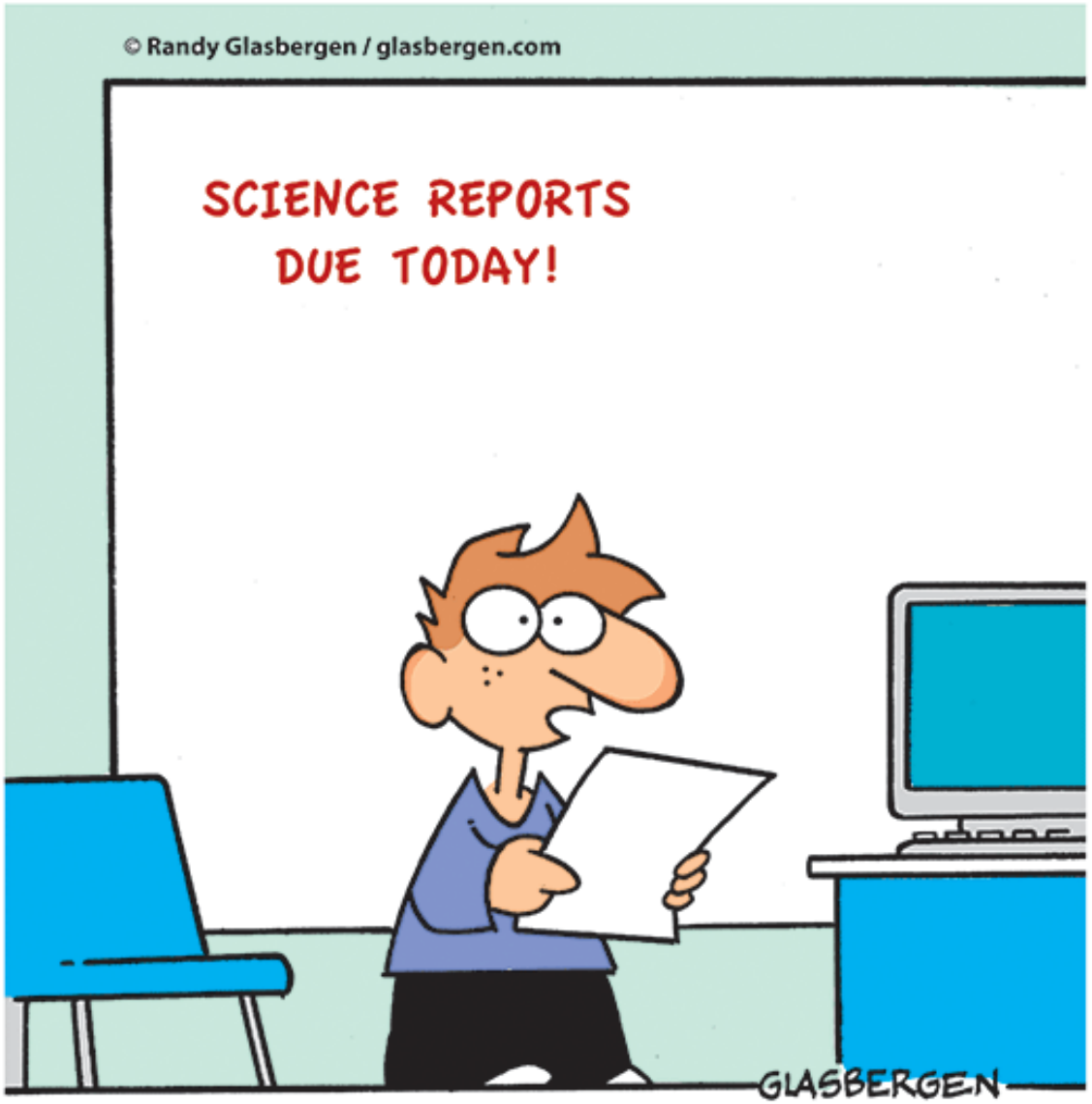
# Privilege Escalation

- @0xNemi discovered a huge cross-OS vulnerability in Intel and AMD processor architecture that leads to privilege escalation with a simple “pop SS”
- **Was bigger than Meltdown?**
- An authenticated local attacker could read sensitive data in kernel memory, control low-level operating system functions, or panic the system
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8897


APTs
Attack Surfaces are Everywhere


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"


Covert Channels



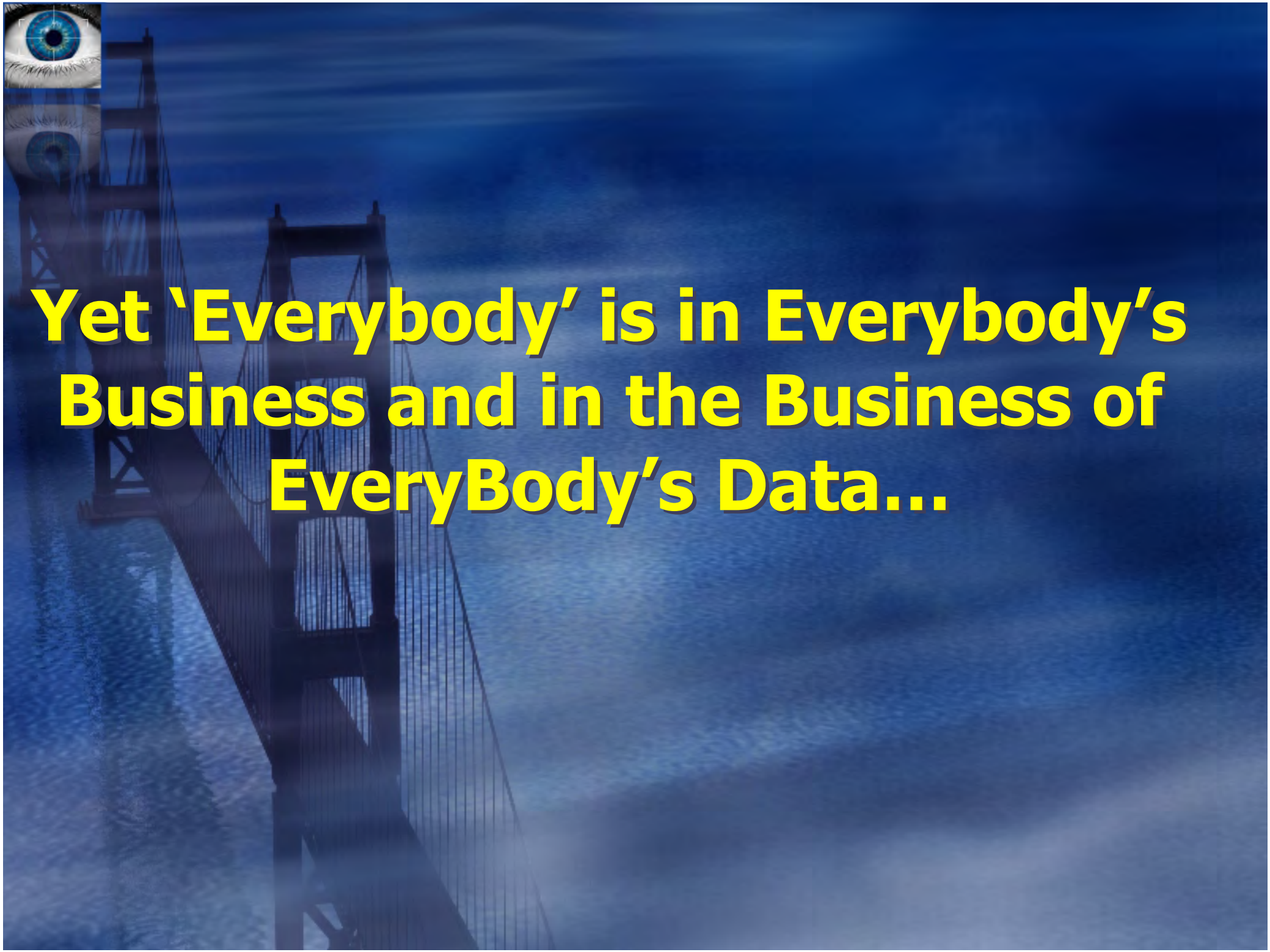

"The left side of the brain contains all of our thoughts, knowledge and memories. The right side is the back-up copy."

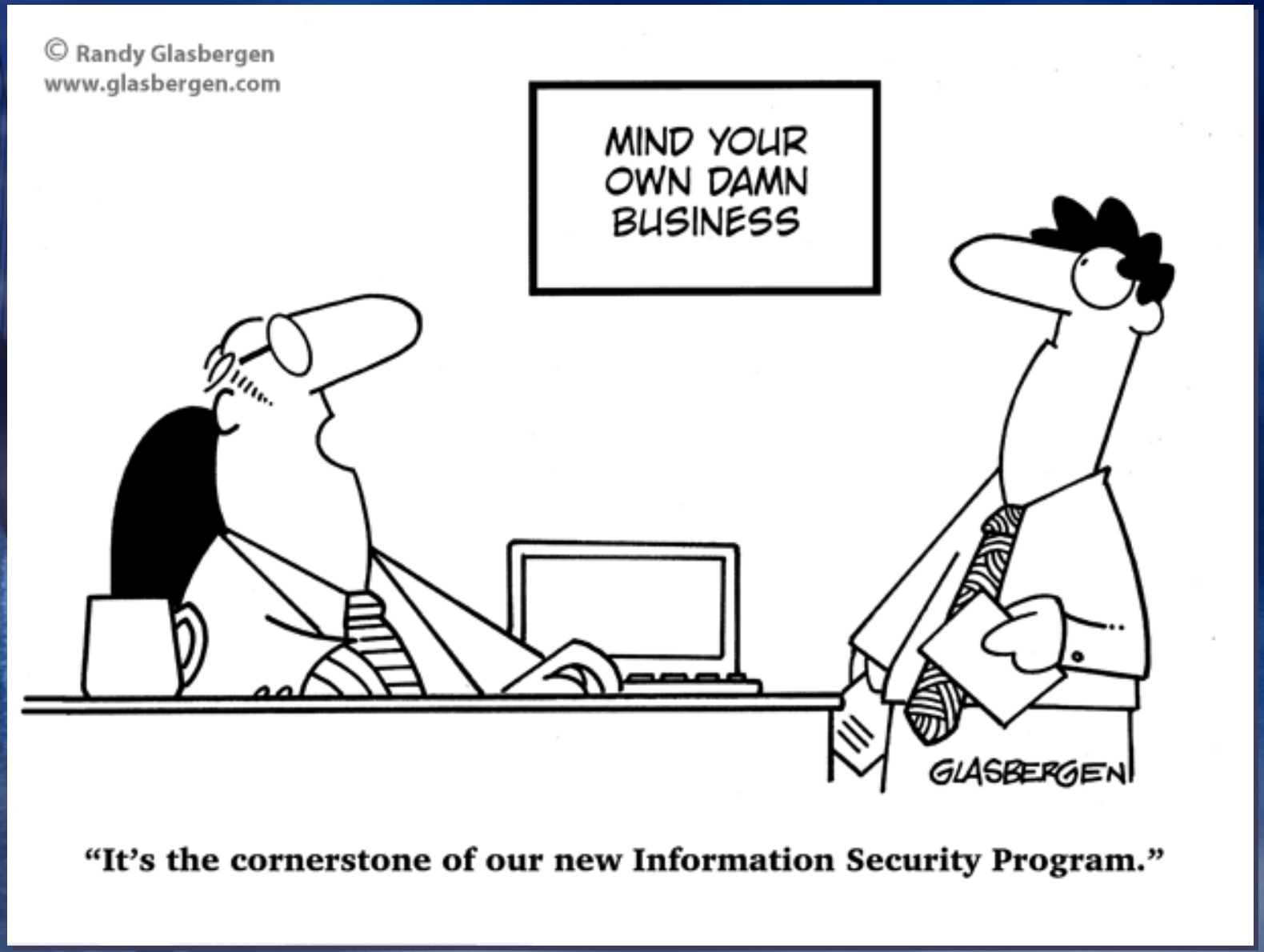
"On the Internet, nobody knows you're a dog."

# Encrypting You?!

There are three kinds of authentication factors:

- What you know (password/PIN code)
- What you have (key/phone/credit card)
- What you are (fingerprint/face/biometrics)


Yet 'Everybody' is in Everybody's Business and in the Business of EveryBody's Data…

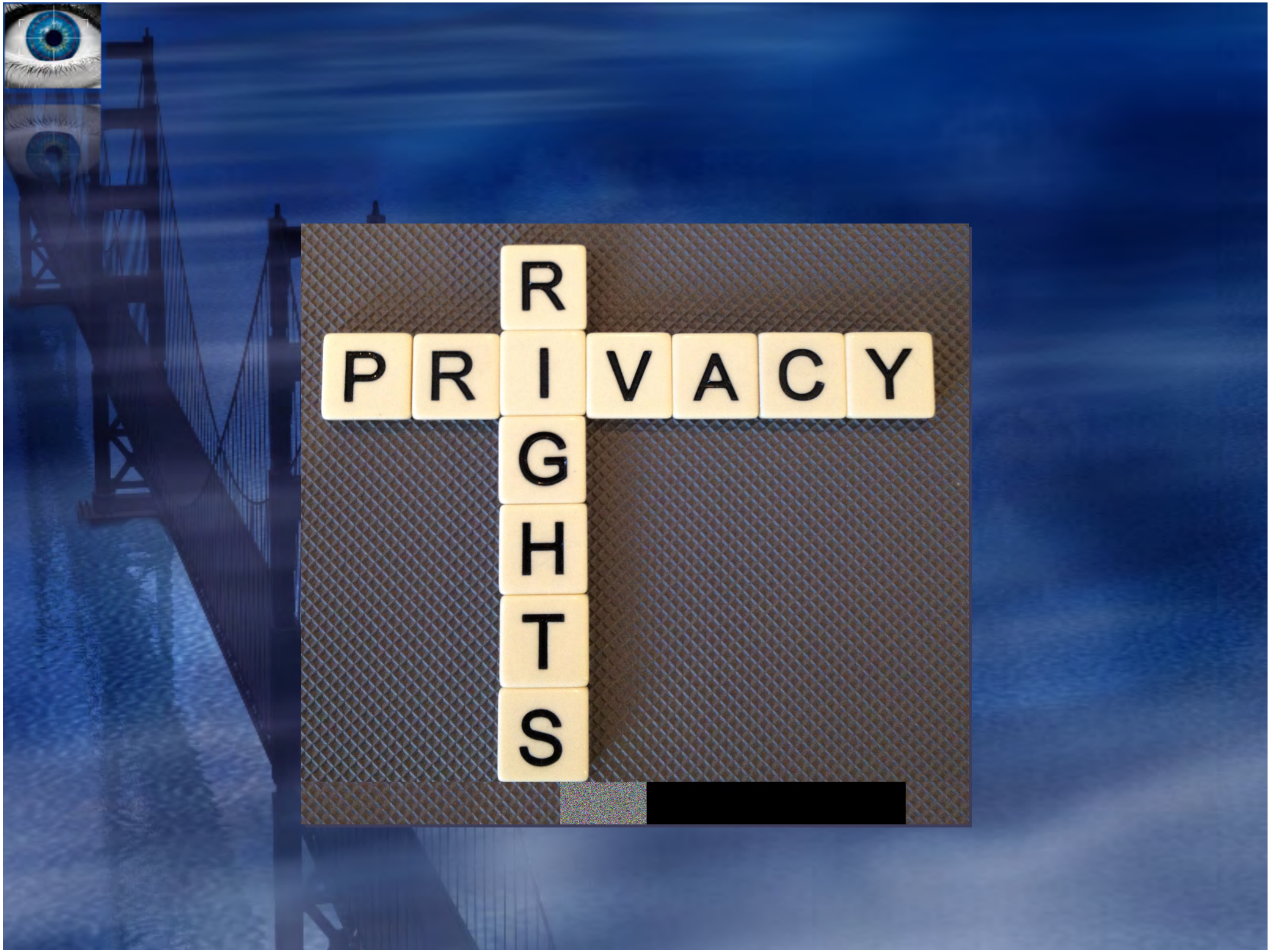



**"It's the cornerstone of our new Information Security Program."**

***Privacide – any privacy is not when the sovereignty of the person, personal space and effects fall under the spell of the persistent gaze…***

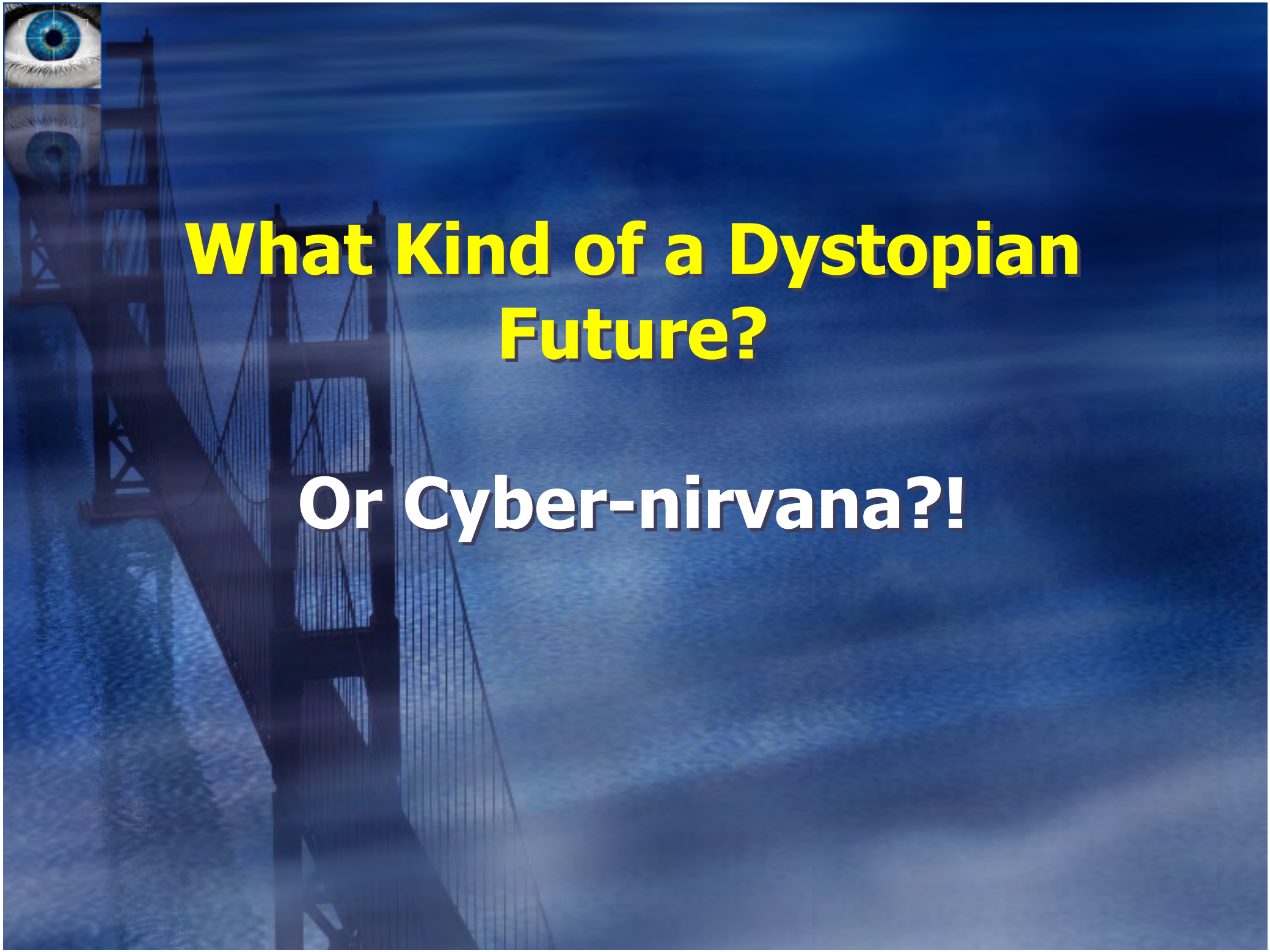
# SecurUS
# REALLY??!!

- Law Enforcement can find location of ANY phone within seconds
- Carriers selling out their subscribers
- No reasonable expectation of privacy
- Third Party Doctrine
- Selling access and selling out your sovereignty
- But nothing to worry about if you have nothing to hide??


PRIVACY
RIGHTS


Weaponizing Privacy and
Persona Information

# Dark Side of Personal Data…
# So Imagine for the Moment…


What Kind of a Dystopian Future?
Or Cyber-nirvana?!

# Context Setting

- ✓ Data absent context is data with no meaning!
  - ✓ And all data is value laden!

- ✓ Lose the context, make up the meaning – incredibly seductive to manage and manipulate data – and for other ends.

- ✓ What do you do with your data?!
- ✓ *How do you frame your data?!*

# The Information Age: Change

**Intelligence was once a "closed" ballgame**

- ✓ Spies
- ✓ Secret electronic surveillance of the radio waves
- ✓ "Private" networks

***- Large, "open" networks – like the Internet – are changing the game***

***- Cheap - increasingly widespread and available***

***- Increasingly easy to "hide"***

**"No secrets worth knowing on Internet!"**

# More challenges…

- ✓ Major problem regarding information sharing
- ✓ Knowledge is control for some – and controlling the data avoids potential competition and loss of power
- ✓ **"What I know data that you don't know data" -- "coin of the realm" – *information hoarding***
- ✓ Human factors as well as institutional and organizational operating behaviors had become major obstacles

# Even More Challenges…

- ✓ **Small vs. Massive Data**
  - ✓ *Huge differences in required approaches, emphasizing statistical approaches and classical RDBMS failing in massive environments*
  - ✓ *Yet industry STILL wants to sell "not invented here" solutions to increase the bottom line and government STILL wants large, multi-billion dollar, multi-year contracts*
- ✓ **Classical query systems required compute-intensive solutions**
  - ✓ *Include key word searches, logic trees, ontologies, entity extraction, etc.*
  - ✓ *All are "weak" in that they incur increased processing costs with many false positives – unless everything is suspicious*
- ✓ **Complex AI queries/data mining is hard, time-consuming work.**

# We're Falling Way Behind…

- ✓ Default approach to access: Pre-select source data (immediate bias)
- ✓ Analyst queries are essentially "stabs in the dark"
- ✓ Data spilling on the floor…
- ✓ Missing all kinds of real-time and stored info and intelligence
- ✓ The magic algorithm – AI

- ✓ *Classic approaches are utterly failing*
- ✓ *Losing the battle with massive data*
- ✓ *Need a "smarter" approach –*
- ✓ *Must consider data in 3 dimensions just not 2!*
  - ✓ *- The missing 'Z' axis…*

# Rise of the National Security Surveillance State

## *GovCo, Inc*

**How is your data being used or bused?**

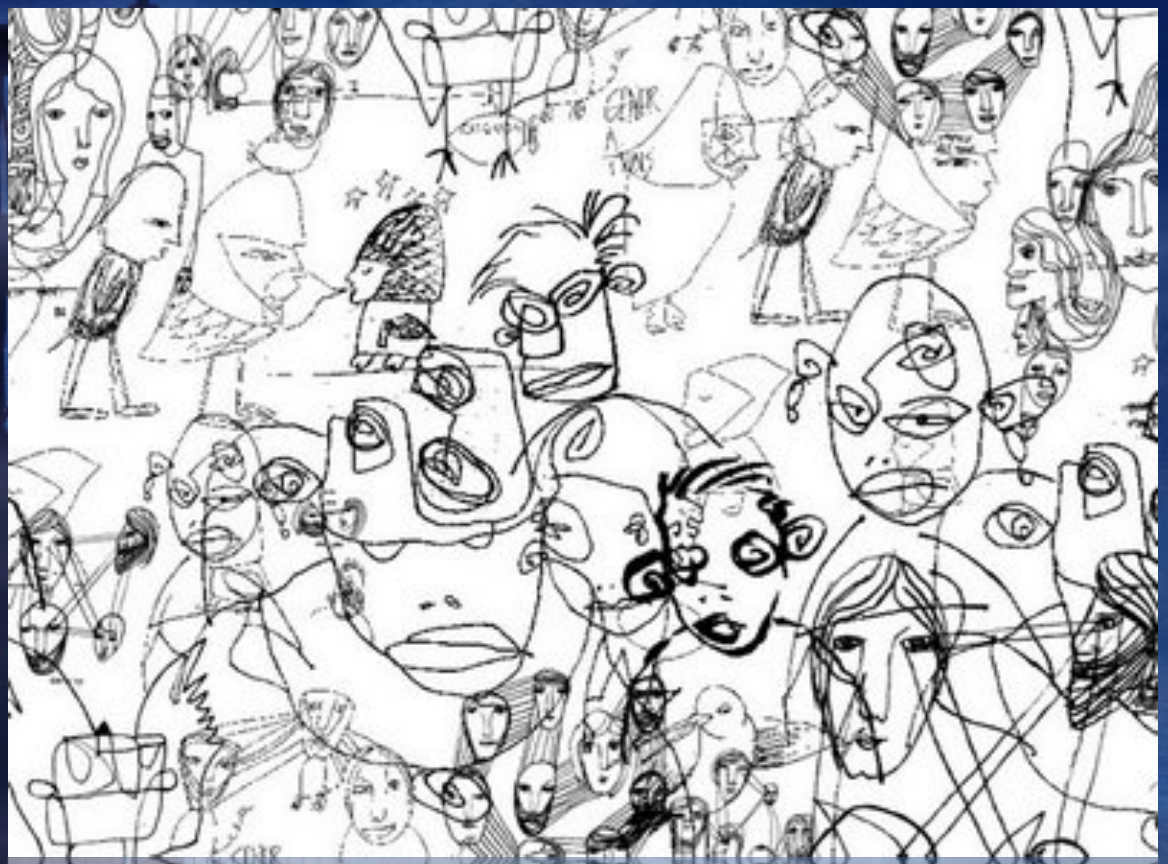
**How do you 'frame' your data?!**

**Do You Know Where Your Data is Today?**

**Or Where it Went Yesterday?**

**Or Where it is Going Tomorrow?!**

# What Do We Do?



# What Do We Do?

***Is it an advancement in our society to give up our privacy because we are so enamored with technology and want advertisers to "market us" with all the digital data 'we 'give them and 'they' have on us – opted in or not?***

***There is an obvious and looming dark side to it as well. So let's not kid ourselves.***

***Industry self-regulation has decidedly NOT worked, and there is no effective, preferably "universal with only specifically designated exceptions" opt out.***

***And we all know that the great convenience and efficiency of the internet has spawned its own dark side -- the spam, the multitude of computer security problems that bedevil us and the insecurity of the infrastructure today.***

# What Do We Do? – Part 2 and You!

## Data as a Weapon?
## Internet as the Delivery Platform?

# What Do We Do? – Part 3

***With the cloud and so much other data other there, the more the data the more it enables the Leviathan state when placed in the wrong hands…***

***… like letting police and government quietly demand all our records without the inconvenience of a surreptitious entry or remote installation of monitoring technology, taking the current warrantless intrusions a step even further.***

***What tale do we want to tell to future generations?***

# *Remember…*

- ✓ Industrial Age versus Information and Knowledge Age world views
  - ✓ Highly disruptive…
- ✓ Social ‘data’ structures… Who owns the data? *Data sovereignty or sovereignty over the data?*
- ✓ Moving from transactional and stove piped to relational and networked
- ✓ *The thinking that got us here today is insufficient for what we need tomorrow*

- with thanks to Einstein

# More challenges…

- ✓ Major problem regarding information sharing
- ✓ Knowledge is control for some – and controlling the data avoids potential competition and loss of power
- ✓ "What I know data that you don't know data" -- "coin of the realm" – *information hoarding*
- ✓ Human factors as well as institutional and organizational operating behaviors have become major obstacles

# Additional Ethical and Practical Implications

- Companies will be forced to deal with a clear conflict of interest between the pursuit of profit and fulfilling a regulatory role on behalf of the government.
- A company will find it difficult to maintain the integrity of its paying customers, especially with respect to their privacy.
- Increasing access to and manipulation of data makes it inherently less secure.
- Changing and vague demands from government might make it difficult to build appropriate data security infrastructure

# Issues with Private Sector Collecting and Storing Data

- Creation of data honeypots
- Data sovereignty issues
- Private sector performing public work – conflicts of interest between profit and surveillance


"Do we really need to encrypt our data? Most of our communications are impossible to understand in the first place."

# Privacy Exercise

## *Making it Personal*

# What Future Do You Want to Keep?

# What Future Do We Want to Keep?

***It's also a case of what the latest technology can do to our privacy and what happens to our very freedom in the wrong hands ...***

***Only the government can create a police state, and our technology can now make that happen.***

***I challenge you all to demand accountability, to update our protections in the Internet Age...***

***Do you care? What will you do about it?***

# Remember Rogue One?
# There Still IS Hope!?