PRIVACY ON THE INTERNET / HEALTH

Security and privacy of HIS

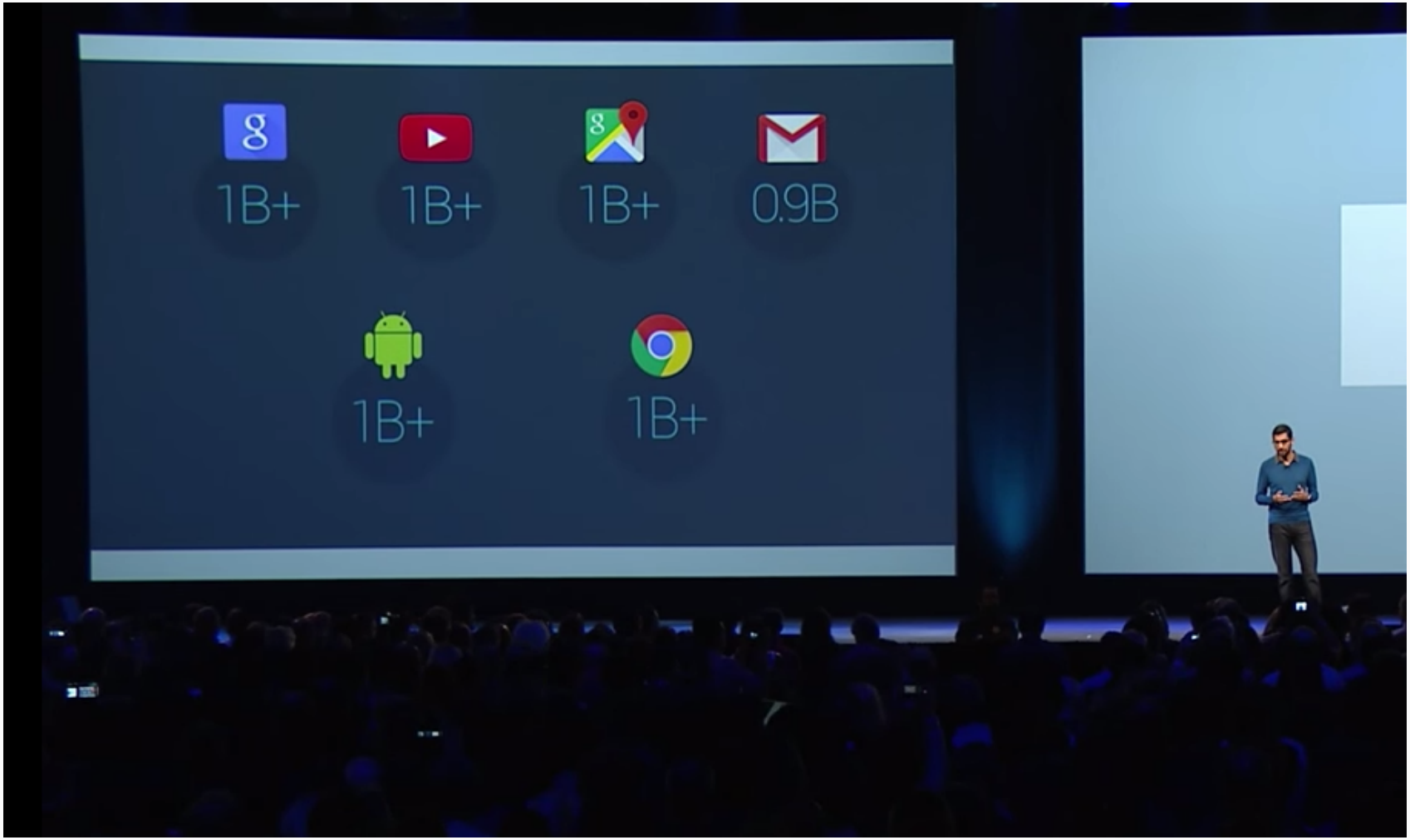
Georgios Spathoulas

Msc in ”Informatics and computational bio-medicine”

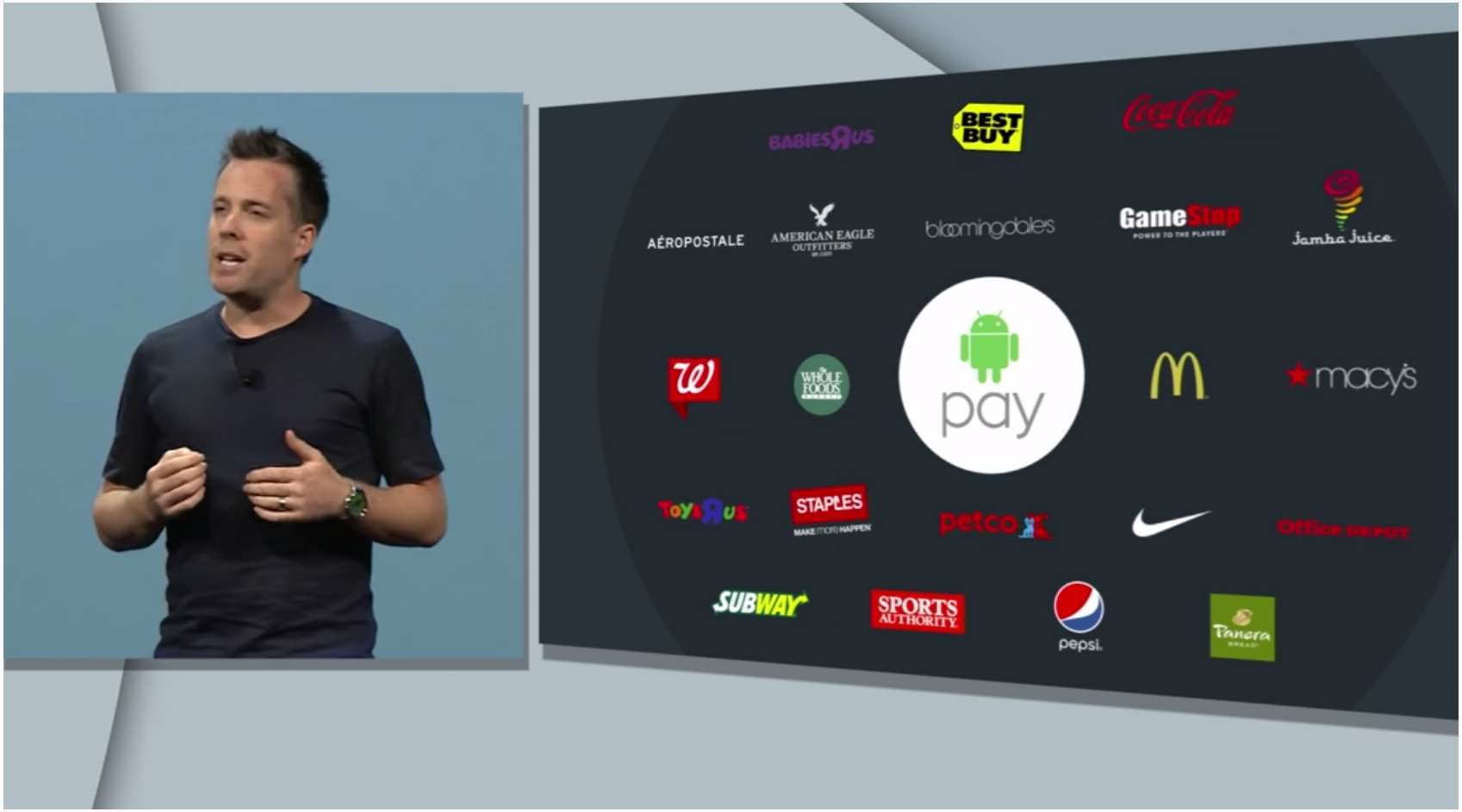
University of Thessaly

GOOGLE I/O 2015

BILLIONS OF USERS

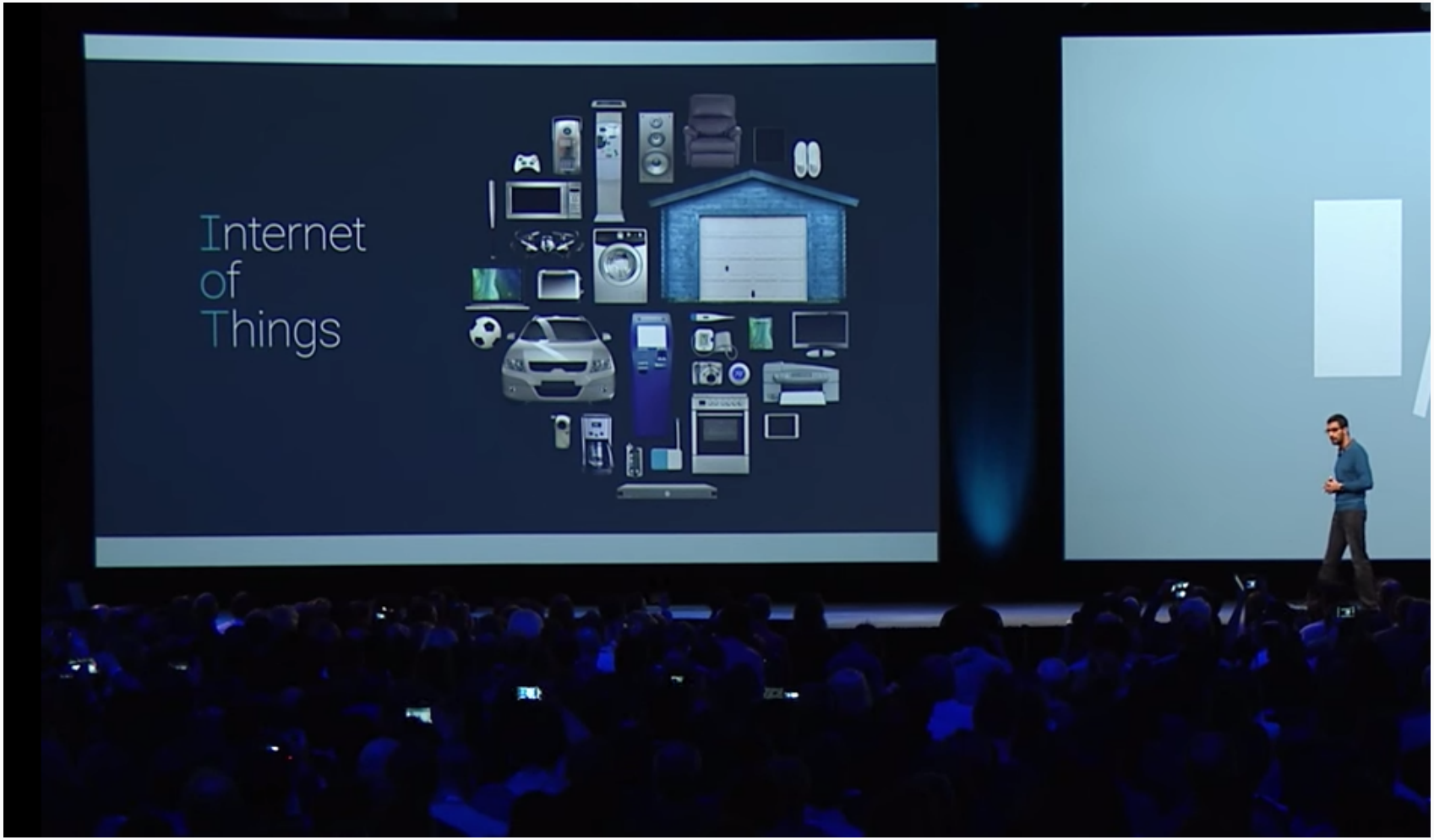


ANDROID PAY

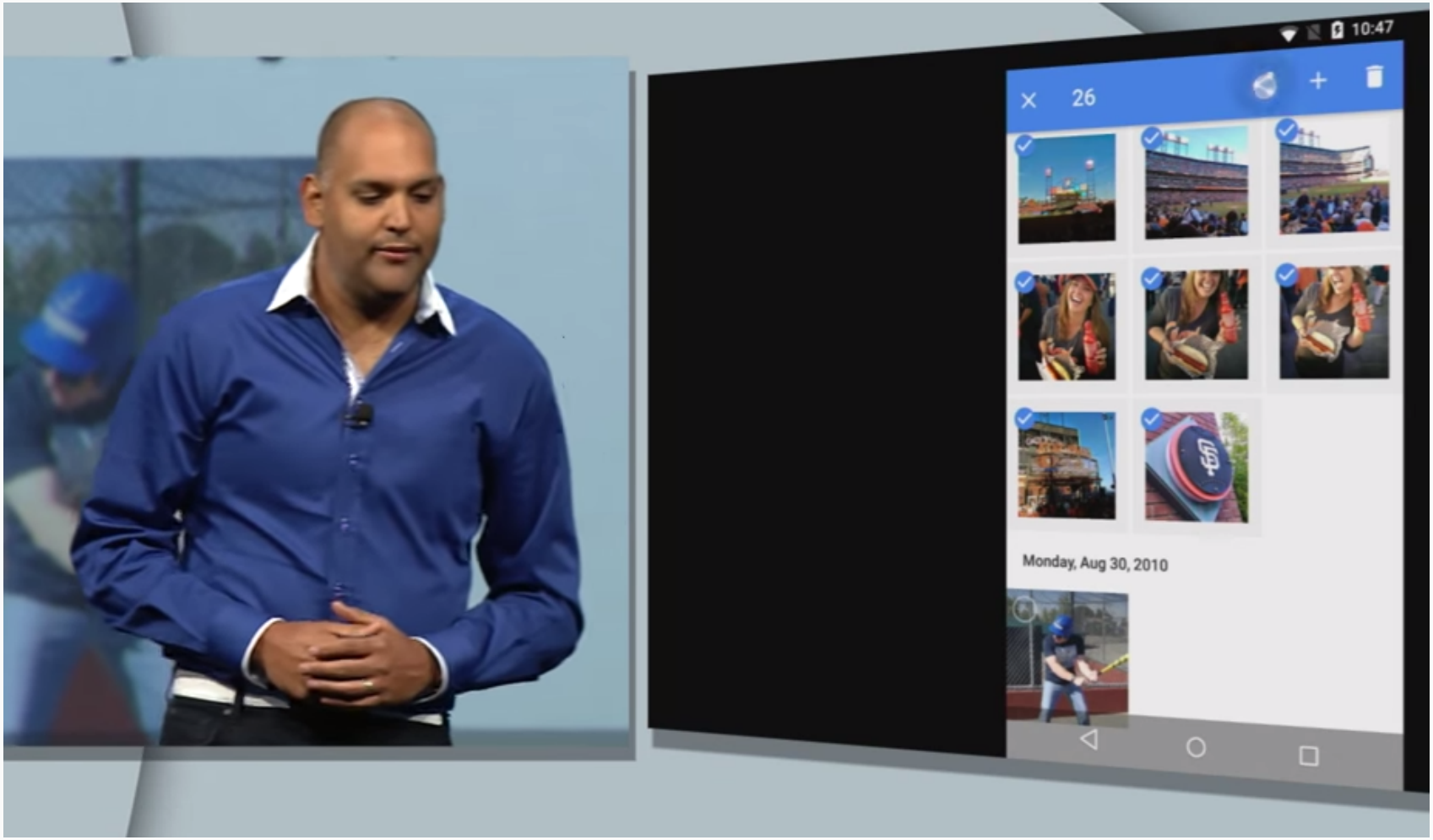

BABIES R US
BEST BUY
Coca-Cola
AÉROPOSTALE
AMERICAN EAGLE OUTFITTERS
bloomingdale's
GameStop
POWER TO THE PLAYERS
Jamba Juice
WHOLE FOODS
pay
macy's
TOYS R US
STAPLES
MAKE more HAPPEN
petco
Office DEPOT
SUBWAY
SPORTS AUTHORITY
pepsi
Panera

ANDROID WEAR

INTERNET OF THINGS



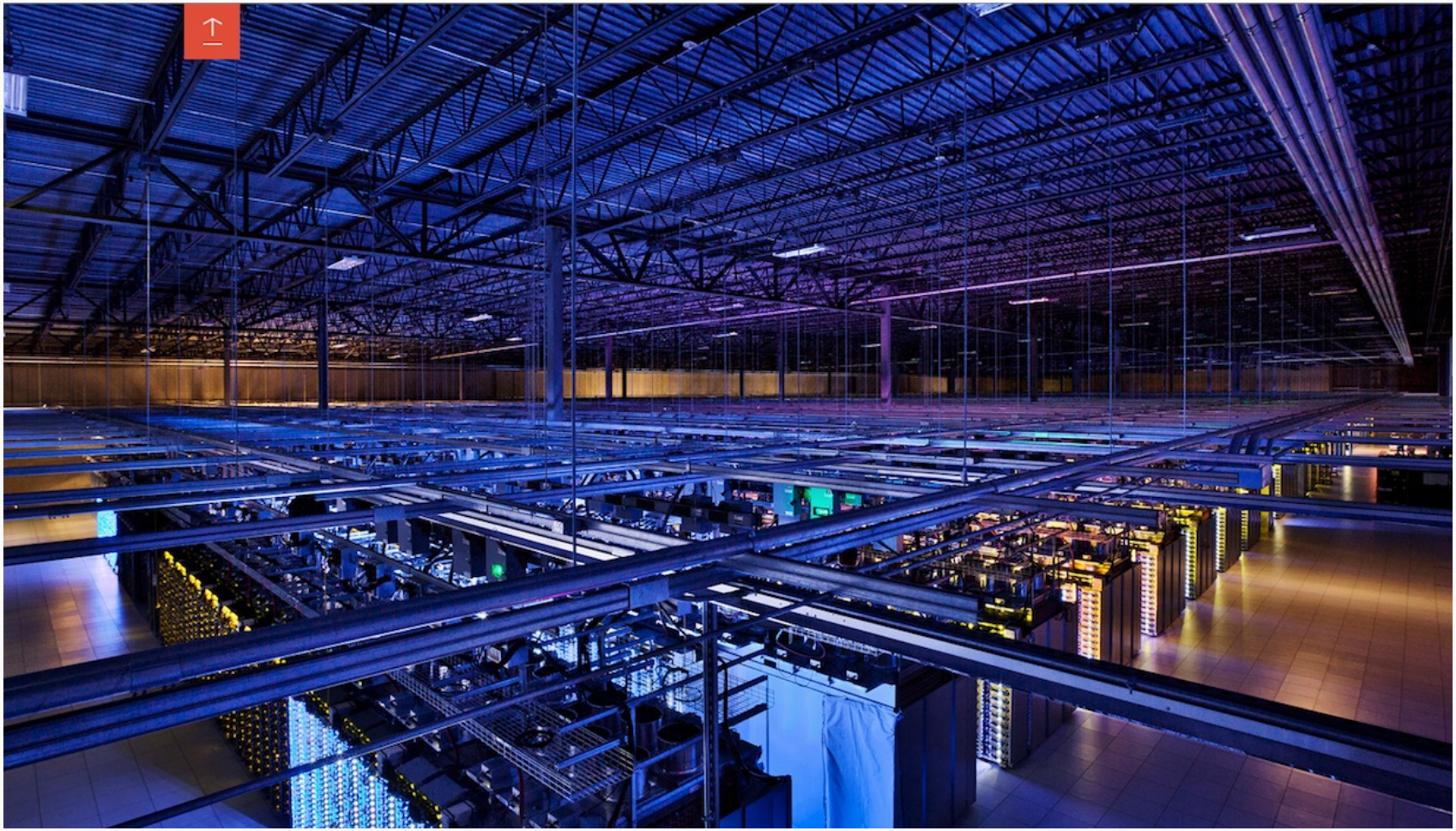
PHOTOS



EVERYONE SHOULD HAVE A PHONE

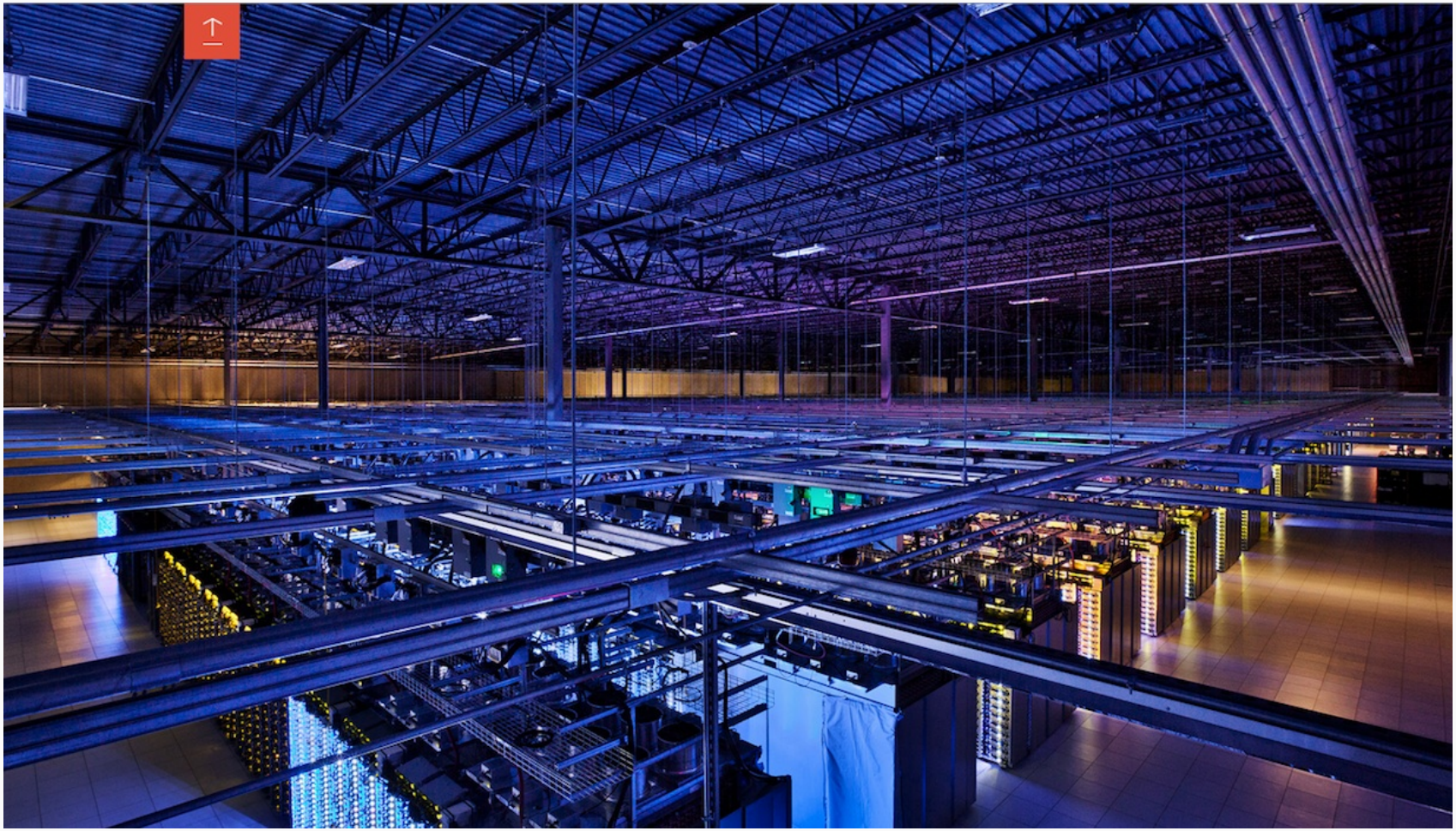
UNDER THE SURVEILLANCE OF CORPORATES

LET'S TALK ABOUT MONEY



Google spends 4 B $ on data centers every quarter

LET'S TALK ABOUT MONEY



Google spends 4 B $ on data centers every quarter
They still make 12 B $ every quarter

ADVERTISING ON TWITTER

ADVERTISING ON TWITTER

ADVERTISING ON TWITTER

ADVERTISING ON TWITTER

+6987635477

HOW MUCH ALL THIS WORTH

HOW MUCH ALL THIS WORTH

facebook

HOW MUCH ALL THIS WORTH

facebook

22 B $

... THE BIGGEST LIE ON THE INTERNET

... do all these corporates act illegally ?

... THE BIGGEST LIE ON THE INTERNET

... do all these corporates act illegally ?

... the biggest lie we all tell will using the Internet is ...

... THE BIGGEST LIE ON THE INTERNET

... do all these corporates act illegally ?

... the biggest lie we all tell will using the Internet is ...

... I have read the license agreements and I agree ...

IT IS ALL ABOUT ADVERTISING

... finally this is all about adverting

IT IS ALL ABOUT ADVERTISING

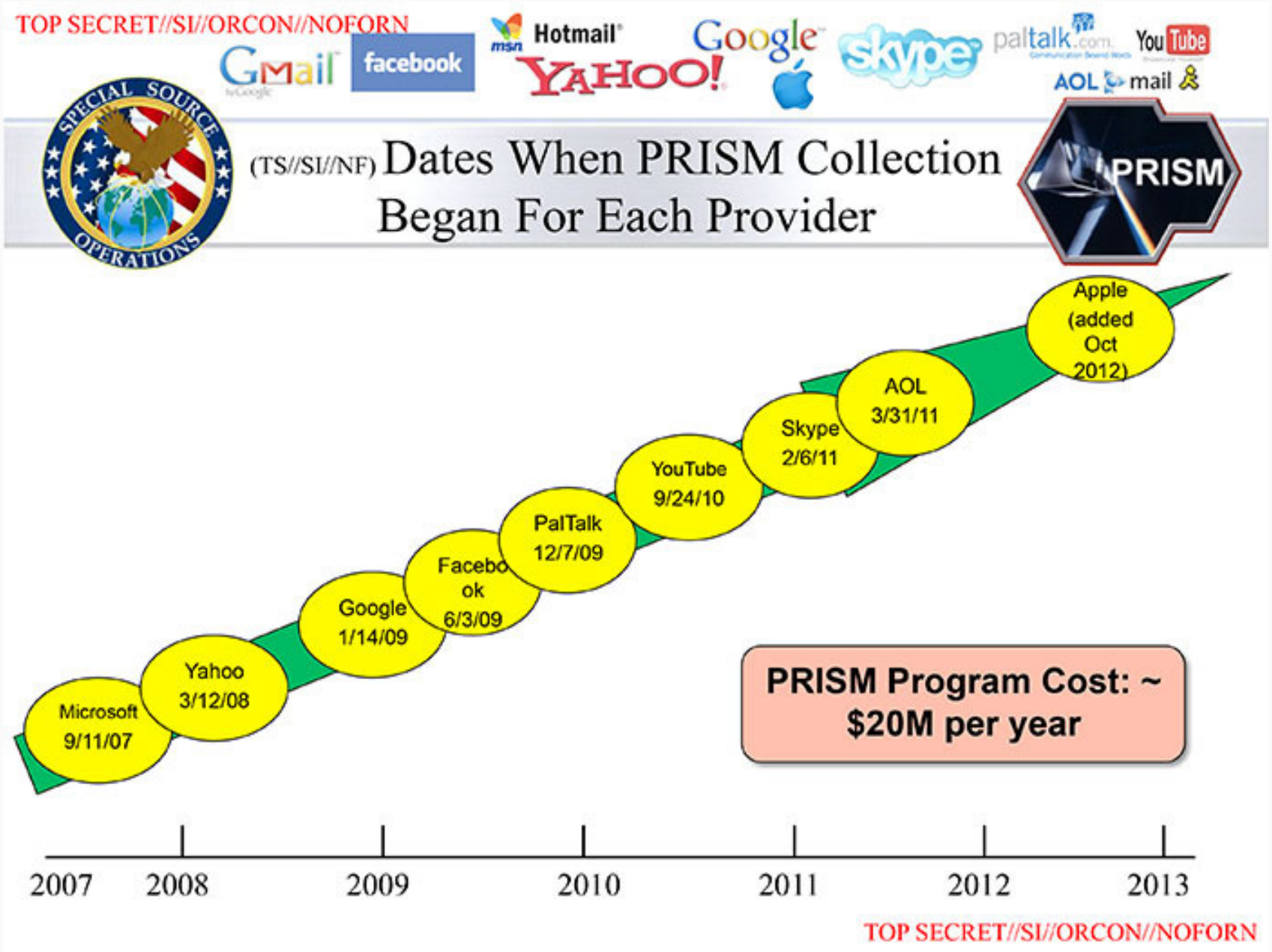
... finally this is all about adverting

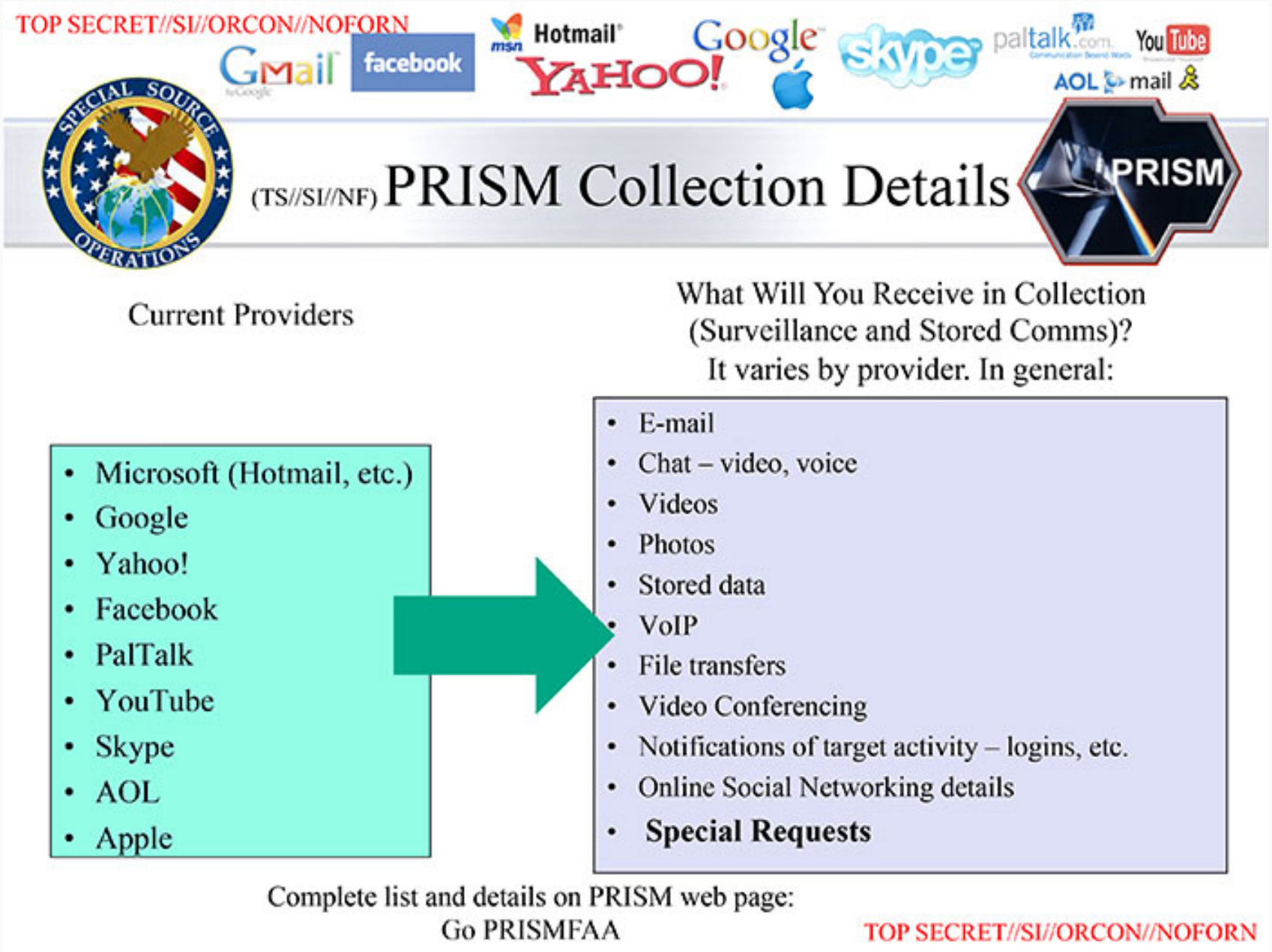
... or is it not ?

UNDER THE SURVEILLANCE OF GOVERNMENTS

ERIC SNOWDEN

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
• Microsoft (Hotmail, etc.)
• Google
• Yahoo!
• Facebook
• PalTalk
• YouTube
• Skype
• AOL
• Apple
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:
• E-mail
• Chat – video, voice
• Videos
• Photos
• Stored data
• VoIP
• File transfers
• Video Conferencing
• Notifications of target activity – logins, etc.
• Online Social Networking details
• Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

…HIDING AWAY…

TOR

WHAT IS THE DEEP WEB?

Put simply, it is the part of the Internet that is hidden from view.

4%
OF WWW CONTENT

SURFACE WEB

Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.

96%
OF WWW CONTENT

DEEP WEB

Also known as the 'Invisible Web', it is the content that cannot be indexed by search engines. And it is hard to keep track of.

The Deep Web is estimated to be **500X** the size of the Surface Web.

SILK ROAD


Silk Road
anonymous marketplace
messages(0) | orders(0) | acc
Shop by category:
Drugs(688)
Cannabis(269)
Ecstasy(36)
Dissociatives(7)
Psychedelics(68)
Opioids(68)
Stimulants(52)
Other(100)
Benzos(46)
Lab Supplies(3)
Digital goods(84)
Services(47)
Money(46)
Weaponry(7)
Home & Garden(27)
Electronics(8)
Books(36)
Drug paraphernalia(27)
XXX(26)
Medical(4)
Computer equipment(8)
Art(1)
Musical instruments(4)
Tickets(3)
Forgeries(10)
$50 Aussie Note! For BitCoin high...
฿5.81
10mg 2C-E Powder
฿0.34
Codeine - 40 x 10MG Codeine/APAP...
฿2.09
Mr. Ouid
Red Joker Ecstasy Pills (Qty:...
฿4.00
BD
Insulin Syringes
Syringes, Needles - 30 Guage 1cc/ml...
฿2.21
0.5g Masterkush melt/bubble hashish...
฿3.19
Mr. Ouid
1-Oz (28g) Purple Kush
an solo
Modafinil 100mg tablets in
Alpha Pharma Testobolin

DEEP WEB

SECURITY AND PRIVACY IN HEALTH

PRIVACY

- **Privacy** is viewed as a **key governing principle** of the patient–physician relationship
- Patients are **required** to **share information** with their physicians to facilitate correct diagnosis and treatment, and to avoid adverse drug interactions
- However, patients may refuse to divulge important information in cases of health problems such as psychiatric behaviour and HIV, as their disclosure may lead to social stigma and discrimination

SIGNIFICANT PERSONAL INFORMATION

Over time, a patient's medical record accumulates significant personal information including :

- identification
- history of medical diagnosis
- digital renderings of medical images
- treatments
- medication history
- dietary habits
- sexual preference
- genetic information
- psychological profiles
- employment history
- income
- physicians' subjective assessments of personality and mental state

HEALTHCARE INFORMATION FLOW

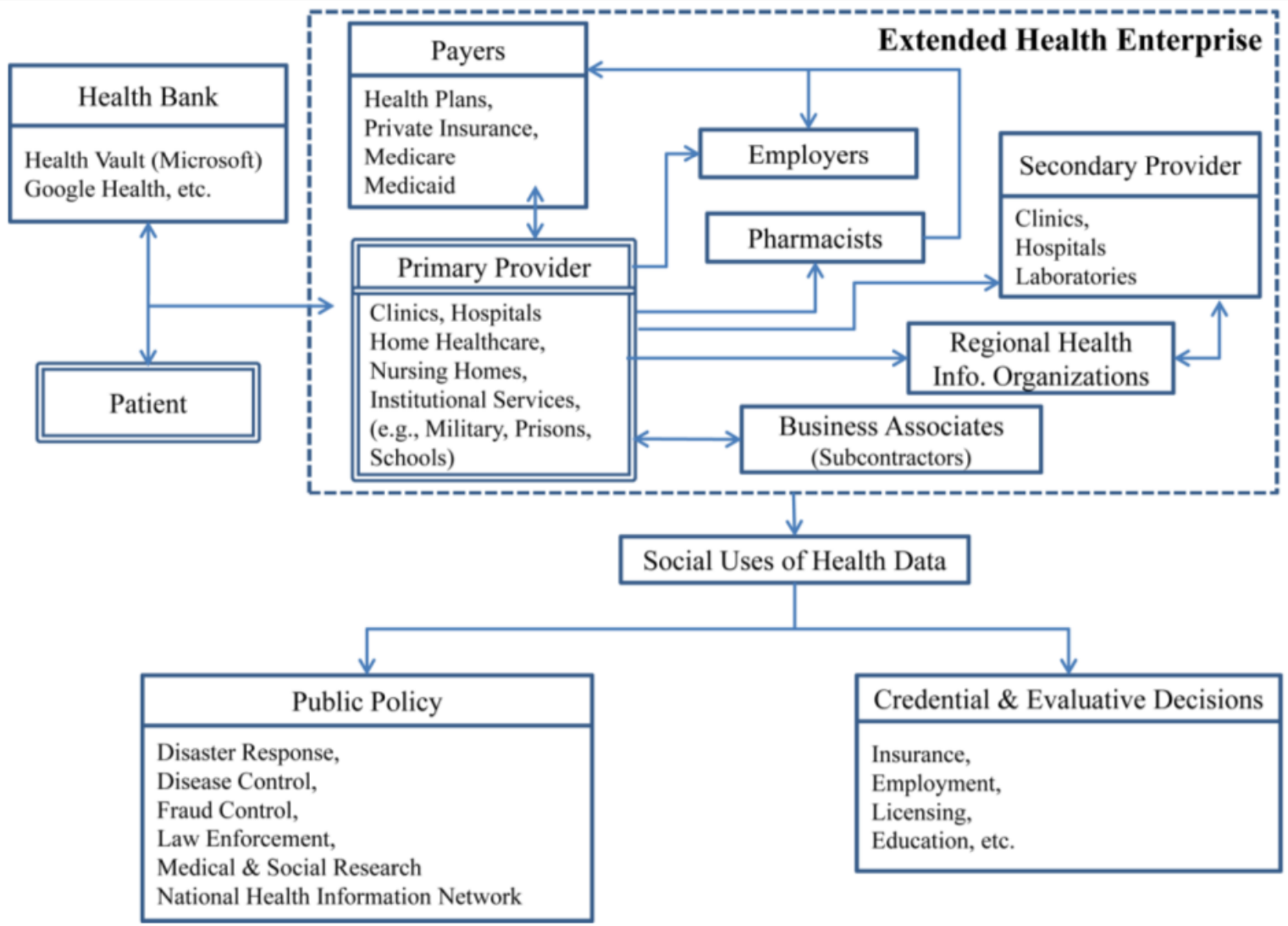


TABLE OF CONTENTS

Threats to Information Privacy

PRIVACY THREATS

Privacy threats broadly categorised into two areas:

- **Organisational threats** that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting a vulnerability of the information systems
- **Systemic threats** that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use

ORGANISATIONAL THREATS

- Organisational threats could be characterised by four components: **motives**, **resources**, **accessibility** and **technical capability**
- Depending on these components, different threats may pose different levels of risk to an organisation requiring different mitigation and prevention strategies
- The motives behind these threats could be economic or non-economic
- These attackers may have resources ranging from modest financial backing and computing skills to a well-funded infrastructure
- Moreover, with the growing underground cyber economy, an individual possessing adequate financial resources and with the intent to acquire data may be able to buy the services of sophisticated hackers to breach healthcare data

LEVELS OF ORGANIZATIONAL THREATS

- **Accidental disclosure:** Healthcare personnel unintentionally disclose patient information to others (e.g., e-mail message sent to wrong address or inadvertent web-posting of sensitive data)
- **Insider curiosity:** An insider with data-access privilege pries upon a patient's records out of curiosity or for their own purpose
- **Data breach by insider:** Insiders access patient information and transmit it to outsiders for profit or revenge
- **Data breach by outsider with physical intrusion:** An outsider enters the physical facility either by coercion or forced entry and gains access to the system.
- **Unauthorised intrusion of network system:** An outsider, including former employees, patients, or hackers, intrudes into an organisation's network from the outside to gain access to patient information or render the system inoperable

SYSTEMIC THREATS

- A major threat to patient privacy occurs, not from outside of the information flow chain, but from **insiders** who are **legally privileged to access patient information**
- For example, insurance firms may deny life insurance to patients based on their medical conditions, or an employer having access to employees' medical records may deny promotion or terminate employment
- Patients or payer organisations may incur financial losses from fraud including upcoding of diagnoses or for rendering medically unnecessary services

HEALTHCARE CONSUMERS' PRIVACY CONCERN

PATIENTS POINT OF VIEW

- First, patients strongly believe that their information should be s**hared only with people involved in their care**
- Second, patients do identify with the **need of information sharing among physicians**, though HIV patients are less likely to approve sharing of their health information
- Third, many patients who agree to information sharing among physicians reject the notion of **releasing information to third parties**, including employers and family members
- Lastly, the majority of patients who have undergone genetic testing believe that **patients should bear the responsibility of revealing test results** to other at-risk family members

STATS

- A survey found that about **28–35%** of patients are **neutral to their health information** – such as age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment – **being used by physicians for other purpose**
- Only about **5–21%** of patients, however, **expected to be asked** for permission to use their information by their physicians
- Similarly, only about **10%** of the patients **expected to be asked for permission if their doctors used their health information for a wide variety of purposes**, including combining data with other patients' data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals and writing research articles about diseases and treatments

STATS

- Another study investigated the divergence of **perception** among patients towards **different types of personal health record systems** (in an increasing order of technological advancement), including paper-based, personal-computer-based, memory devices, portal and networked PHR
- The study found that patients' **relative perception of privacy and security concern increased with the level of technology**, e.g., relative security and privacy concern for networked PHR is twice that of memory-device-based PHR
- However, technologically advanced PHR systems were found to be favoured by highly educated patients

Information security issues of e-health

HEALTH BANK

- The healthcare sector is experiencing a tectonic shift in enablement of healthcare services through internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access and asset tracking among others
- Recent advances in web technology have enabled new approaches to patient information management such as **Banking on Health** or **Health Bank**
- The notion of a health bank is a platform for storage and exchange of patient health records patterned after a personal banking system where consumers could deposit and withdraw information(Microsoft‘s **Health Vault** is an example)
- However, such web-enabled and mobile-based services open up a whole gamut of security risks compounding the privacy problem

CIRCLE OF TRUST

- A common platform for privacy and security in e-health is needed to establish a **Circle of Trust (CoT)** for cooperating enterprises such as hospitals, pharmacies, labs, and insurers thereby enabling them to offer web-based services to patients
- In this framework, personally identifiable information is managed by a designated **Identity Provider** who provides pseudonymous identities of patients for transactions among partners
- Further, an audit service, provided by an independent organisation, logs all transactional requests made by members of CoT, thus enabling:
  - a privacy officer or regulatory agency to validate privacy compliance or investigate allegations of privacy breaches
  - individual patients to verify how their data is being used and challenge data accuracy

RISKS IN AUTHORISED DATA DISCLOSURE

DATA RELEASE

- In the health-care sector, it is often **necessary to share data** across organisational boundaries to support the larger interests of multiple stakeholders as well as agencies involved with public health
- However, the release of patient data could **entail personally identifying information** as well **sensitive information** that may violate privacy as well cause socio-economic repercussions for patients
- Yet such data, when **masked** for identifying and sensitive information, **must maintain the analytic properties to assure statistical inferences**, especially when released for epidemiological research

DISCLOSURE RISK AND INFORMATION LOSS

- In protecting the confidentiality of patients, the data owners must satisfy two **opposing objectives**: namely the **privacy** of individuals and **usability** of released data
- These two objectives are generally referred to as **disclosure risk** and **information loss**
- An emergent body of research focusing on the development of data disclosure methods, and evaluation of such methods, employs a variety of measures for disclosure risk and information loss

MEASUREMENT OF INFORMATION LOSS

- Disclosure of patient information for research purpose requires that the disclosed data remains consistent with respect to its statistical properties to minimise information
- The measurement of information loss, however, **depends on potential usages of released data**, which is difficult to anticipate **at the time of disclosure**
- For example, some disclosure control methods may alter the multivariate covariance structure of attributes necessary for conducting multivariate regression analyses, while keeping the univariate properties intact

Anthem Data Breach: An Example

THE FACTS

- On **December 10, 2014**, someone compromised a database owned by **Anthem Inc., USA** second largest health insurer
- The compromise wasn't discovered until **January 27, 2015**, after a database administrator discovered his credentials being used to run a questionable query – a query he didn't initiate
- Two days later (**January 29**), **Anthem** alerted authorities and that their internal investigation determined the incident was in fact a data breach
- On February 4, 2015, the company **disclosed** the breach to the **public**

STATEMENT

Anthem President and CEO, **Joseph R. Swedish**, said in a statement

”Anthem was the target of a **very sophisticated external cyber attack**. These attackers gained **unauthorized access** to Anthem’s IT system and have obtained **personal information** from our current and former **members**. Those responsible for the attack were able to obtain personal information from our current and former members such as their **names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data**.”

THE FACTS

- The scope of the breach is not fully understood, but there's a good chance that a **majority** of the **80 million records** contained in the compromised database were exposed
- According to company metrics, one in nine Americans have medical coverage through one of Anthem's affiliated plans.
- Anthem uses **TeraData** for data warehousing, which is a robust platform that's able to work with a number of enterprise applications and has a number of solid security controls available to customers
- In the aftermath of the breach at Anthem, experts have speculated on **whether the data in the database was encrypted** at the time the attackers compromised it
- The problem is that protection goes by the wayside once an attacker compromises an administrator's credentials
- So **even if the data was encrypted**, it didn't matter **once the attacker(s) had total control** over the database

PHISING

- Anthem later confirmed that not only did the incident start last December, but the company also confirmed that **five tech employees had their credentials compromised**
- So while the attackers could have used Java, Windows, or Adobe vulnerabilities, the **fastest** way to obtain credentials is to **ask for them**, which is exactly what **Phishing** does in most cases
- Between **Google, LinkedIn, Facebook**, and various posts across the Web, it wouldn't take long to develop an **email scheme** that would eventually lead someone within Anthem's technology group to **reveal** their **credentials**.

PERSISTENT THREATS

- But the difference between a passive attack that uses Phishing and what happened at Anthem is **persistence**.
- Based on Anthem's defenses, it's possible that they attacker(s) **tried to compromise the database earlier in 2014**, but were thwarted
- However, they kept at it and eventually succeeded. **Generic attacks play the numbers game**, hoping to get victims on volume
- Focused attacks **have a small number of targets**, and keep taking shots until they get a hit.
- While it's possible that legacy systems are in use on the network, or perhaps Anthem was behind on patches or other maintenance, **it does not matter once the credentials have been compromised**

TECHNICAL COUNTER MEASURES

- It will be interesting to discover **of what exactly the DBA's credentials consisted**
- If they were simply a username and a password, shame on Anthem
- Such systems need **two-factor authentication**
- In that case, two-factor authentication might have prevented, or at least made an attack such as the one at Anthem difficult
- But what if the attack was sophisticated enough to capture and maintain a valid authenticated session token in real-time, even with two-factor authentication in place?
- Again, **technical controls will only go so far**

HUMAN ELEMENT OF SECURITY

- Once the **humans are exploited**, those controls are next to useless
- Behavioral controls and monitoring can help flag a compromised human element, but it isn't an exact science
- For example, technology didn't detect the Anthem breach, a human who was paying attention did
- **Self-awareness among the staff is a serious bonus to any information security program**

LECTURES

1. **Introduction** (15/03/2016)
2. **Python workshop I** (22/03/2016)
3. **Python workshop II** (29/03/2016)
4. **Privacy preserving data publishing** (05/04/2016)
5. **Cryptography** (12/04/2016)
6. **Homomorphic encryption** (19/04/2016)
7. **Secure multi-party computing** (10/05/2016)
8. **Disaster recovery** (17/05/2016)
9. **HIS in greek hospitals** (24/05/2016)
10. **Papers presentations** (31/05/2016)

BIBLIOGRAPHY

- **Information security and privacy in healthcare: current state of research**, Ajit Appari and M. Eric Johnson
- **Anthem: How does a breach like this happen?**, Steve Ragan, http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html