Data Security and Data Governance

Foundation and Case Studies

including Privacy, Legal, Social and Ethical Issues

Thiti Vacharasintopchai, D.Eng., ATSI-DX, CISA

November 4, 2020

About Me

D.Eng. (AIT 2007)

M.Eng. (AIT 2000)

B.Eng. (Chula 1998)

Certified Information Systems Auditor (CISA)

ATSI DX expert

#construction
#techmanagement
#realestate
#university
#healthcare

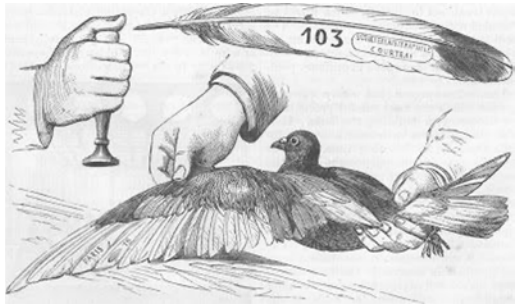
DISCLAIMER

All views expressed are my own and

do not represent the opinions of any entity with which

I have been or am now affiliated

We are living in the ultra-connected world

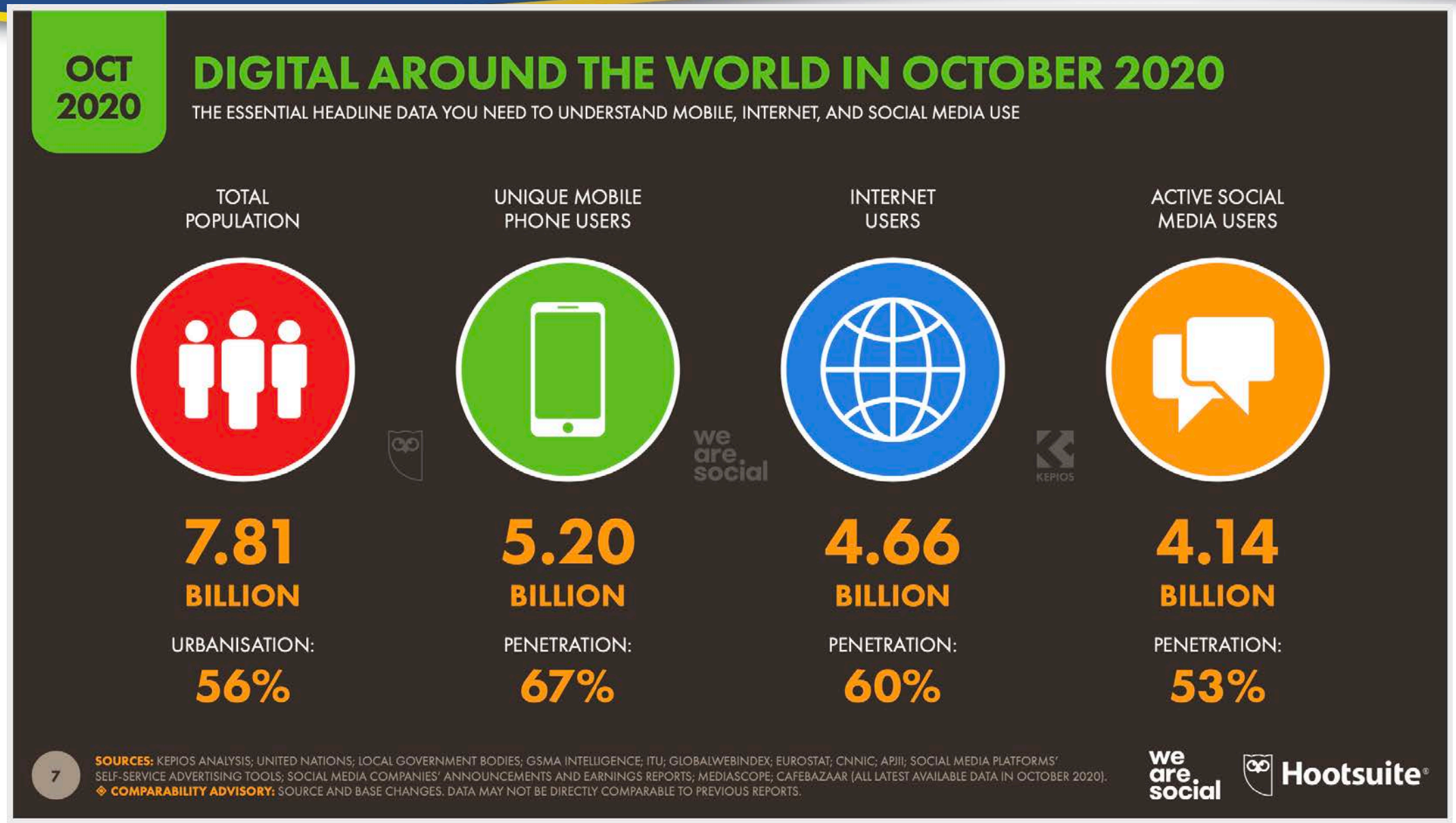


1844 first telegraph

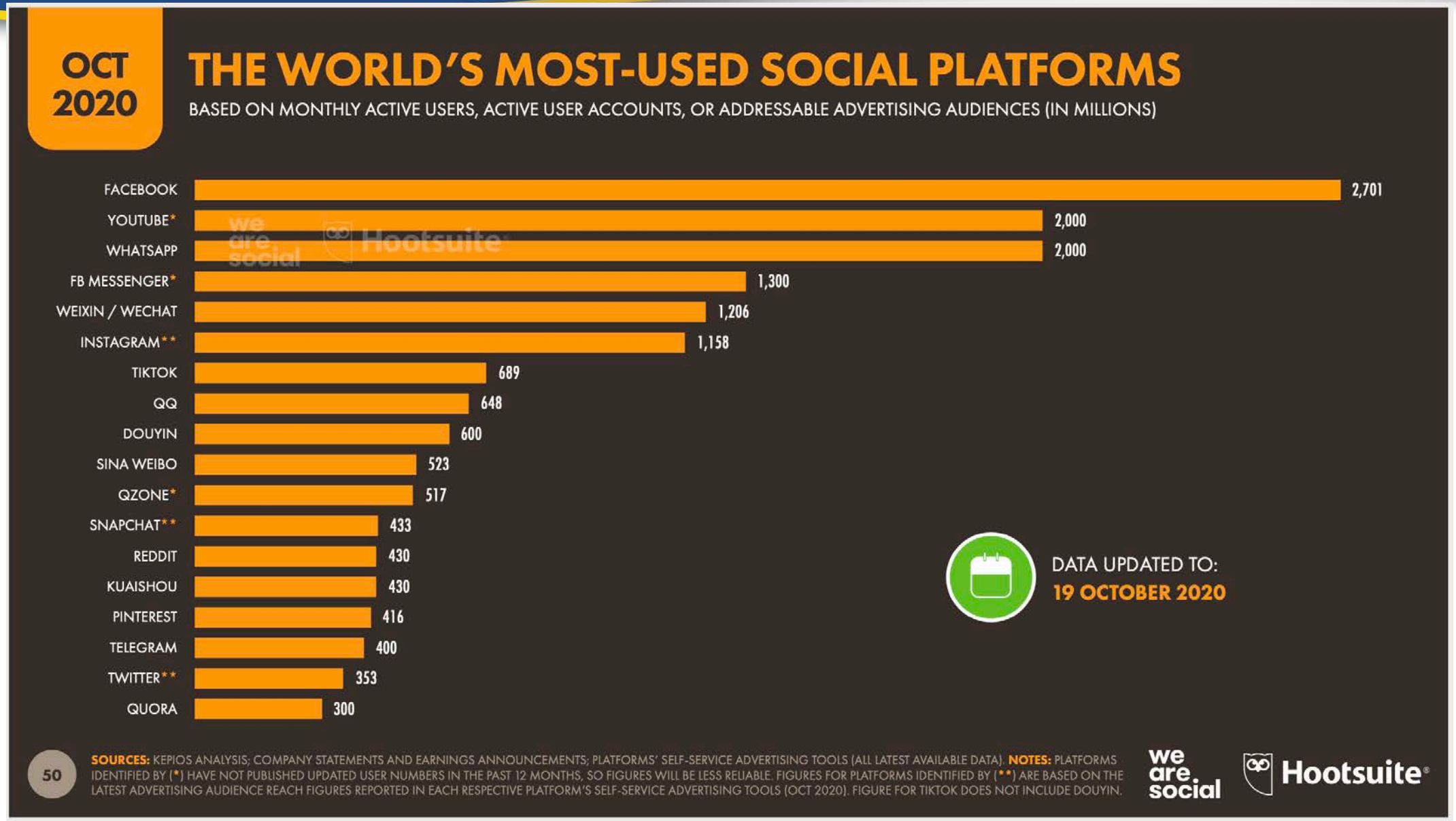
1983

...

2020 5G 4K HDR
on-device ML - ultra personalized



Source: https://hootsuite.com/pages/digital-2020



Source: https://hootsuite.com/pages/digital-2020

OCT 2020

FACEBOOK REACH RANKINGS

COUNTRIES AND TERRITORIES* WITH THE GREATEST POTENTIAL FACEBOOK ADVERTISING REACH

#	COUNTRY	REACH	▲QOQ	▲QOQ
01	INDIA	310,000,000	+7%	+20,000,000
02	U.S.A.	190,000,000	0%	[UNCHANGED]
03	INDONESIA	140,000,000	0%	[UNCHANGED]
04	BRAZIL	130,000,000	0%	[UNCHANGED]
05	MEXICO	92,000,000	+3%	+3,000,000
06	PHILIPPINES	81,000,000	+7%	+5,000,000
07	VIETNAM	65,000,000	+2%	+1,000,000
08	THAILAND	50,000,000	0%	[UNCHANGED]
09	EGYPT	44,000,000	+5%	+2,000,000
10=	BANGLADESH	39,000,000	+3%	+1,000,000
10=	PAKISTAN	39,000,000	+3%	+1,000,000
12	U.K.	38,000,000	+3%	+1,000,000
13	TURKEY	37,000,000	0%	[UNCHANGED]
14	COLOMBIA	36,000,000	+3%	+1,000,000
15	FRANCE	32,000,000	0%	[UNCHANGED]
16	ARGENTINA	31,000,000	+3%	+1,000,000
17	ITALY	30,000,000	0%	[UNCHANGED]
18=	GERMANY	28,000,000	0%	[UNCHANGED]
18=	NIGERIA	28,000,000	+4%	+1,000,000
20	MYANMAR	26,000,000	+4%	+1,000,000

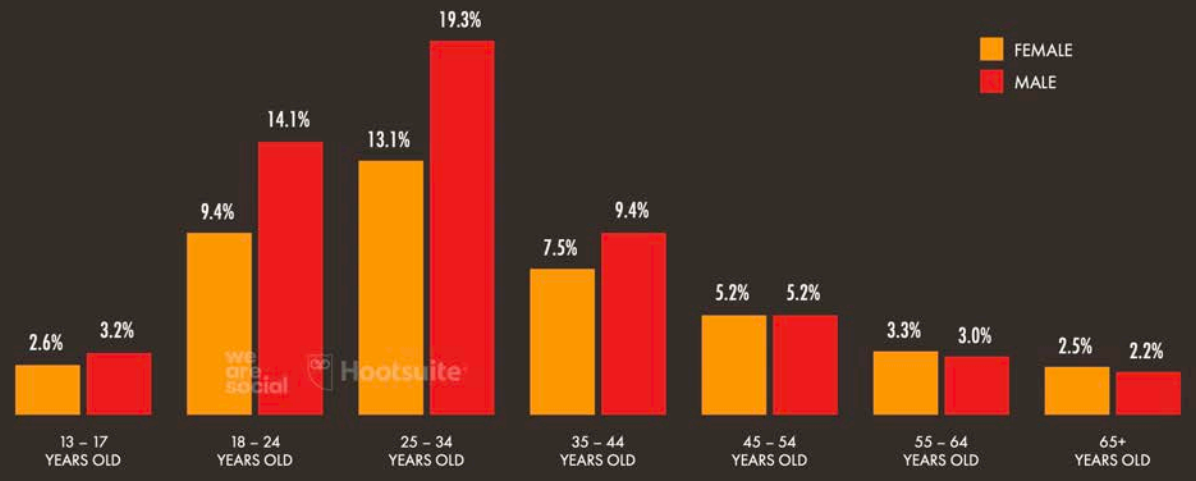
56 SOURCE: EXTRAPOLATIONS OF DATA FROM FACEBOOK'S SELF-SERVICE ADVERTISING TOOLS (OCTOBER 2020). *NOTE: ONLY INCLUDES COUNTRIES AND TERRITORIES WITH POPULATIONS OF AT LEAST 50,000 PEOPLE. ◆ COMPARABILITY ADVISORY: BASE CHANGES.

we are social Hootsuite

OCT 2020

PROFILE OF FACEBOOK'S ADVERTISING AUDIENCE

SHARE OF FACEBOOK'S GLOBAL ADVERTISING AUDIENCE* BY AGE GROUP AND GENDER*

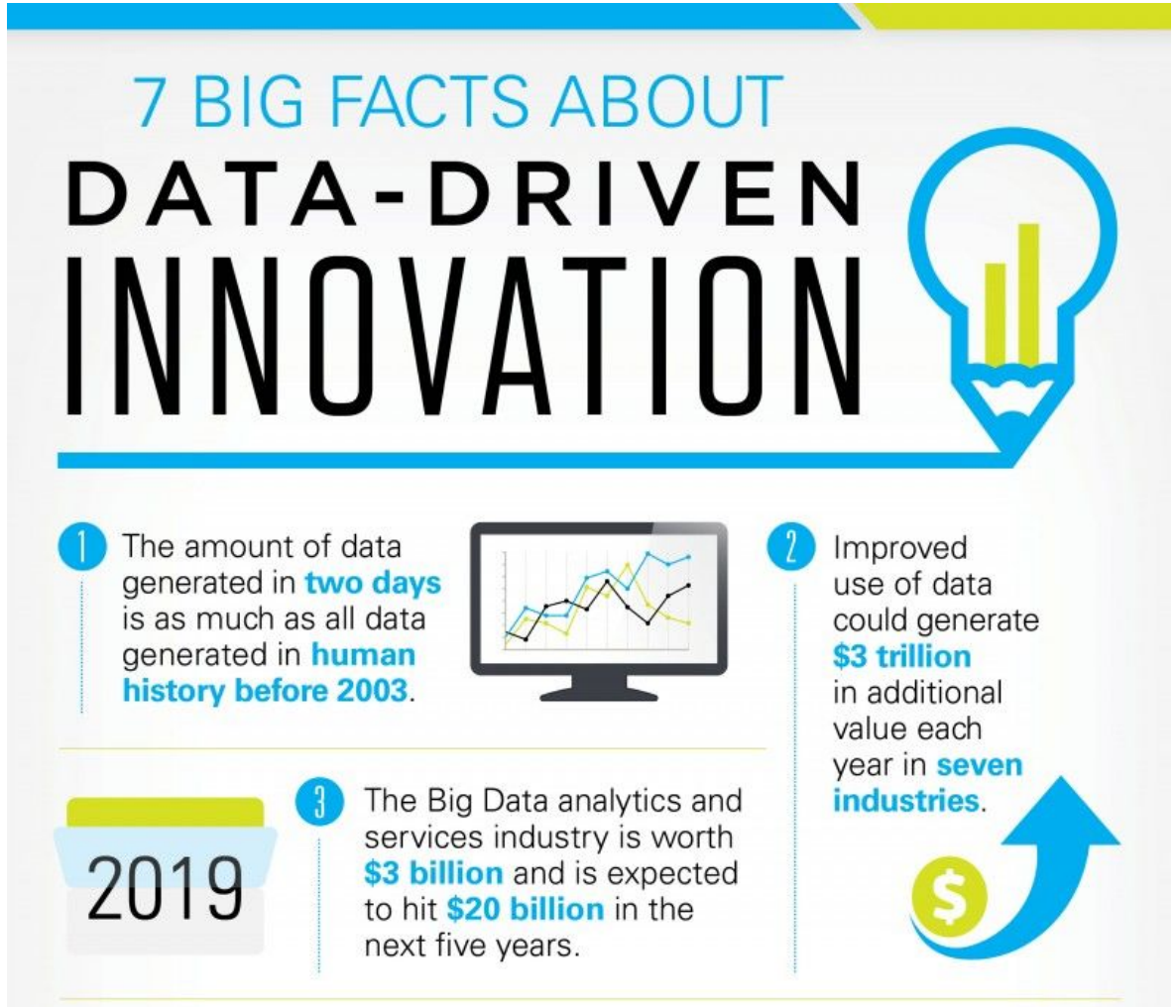


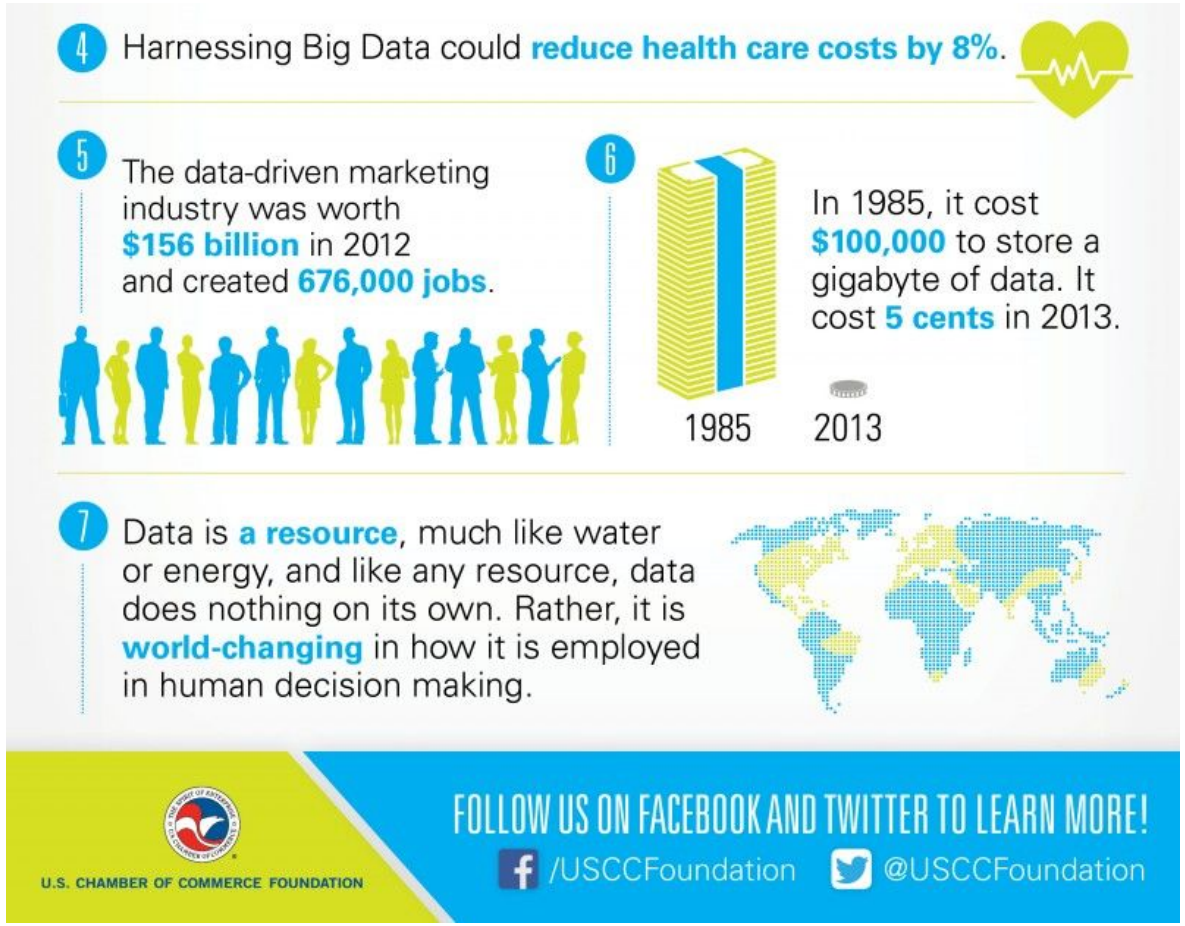
59 SOURCE: EXTRAPOLATIONS OF DATA FROM FACEBOOK'S SELF-SERVICE ADVERTISING TOOLS (OCTOBER 2020). *NOTES: FACEBOOK'S TOOLS DO NOT PUBLISH AUDIENCE DATA FOR GENDERS OTHER THAN 'MALE' OR 'FEMALE'. *ADVISORY: DATA ON THIS CHART REPRESENT FACEBOOK'S ADVERTISING AUDIENCE ONLY, AND MAY NOT CORRELATE TO RESPECTIVE SHARES OF TOTAL MONTHLY ACTIVE USERS. ◆ COMPARABILITY ADVISORY: BASE CHANGES.

we are social Hootsuite

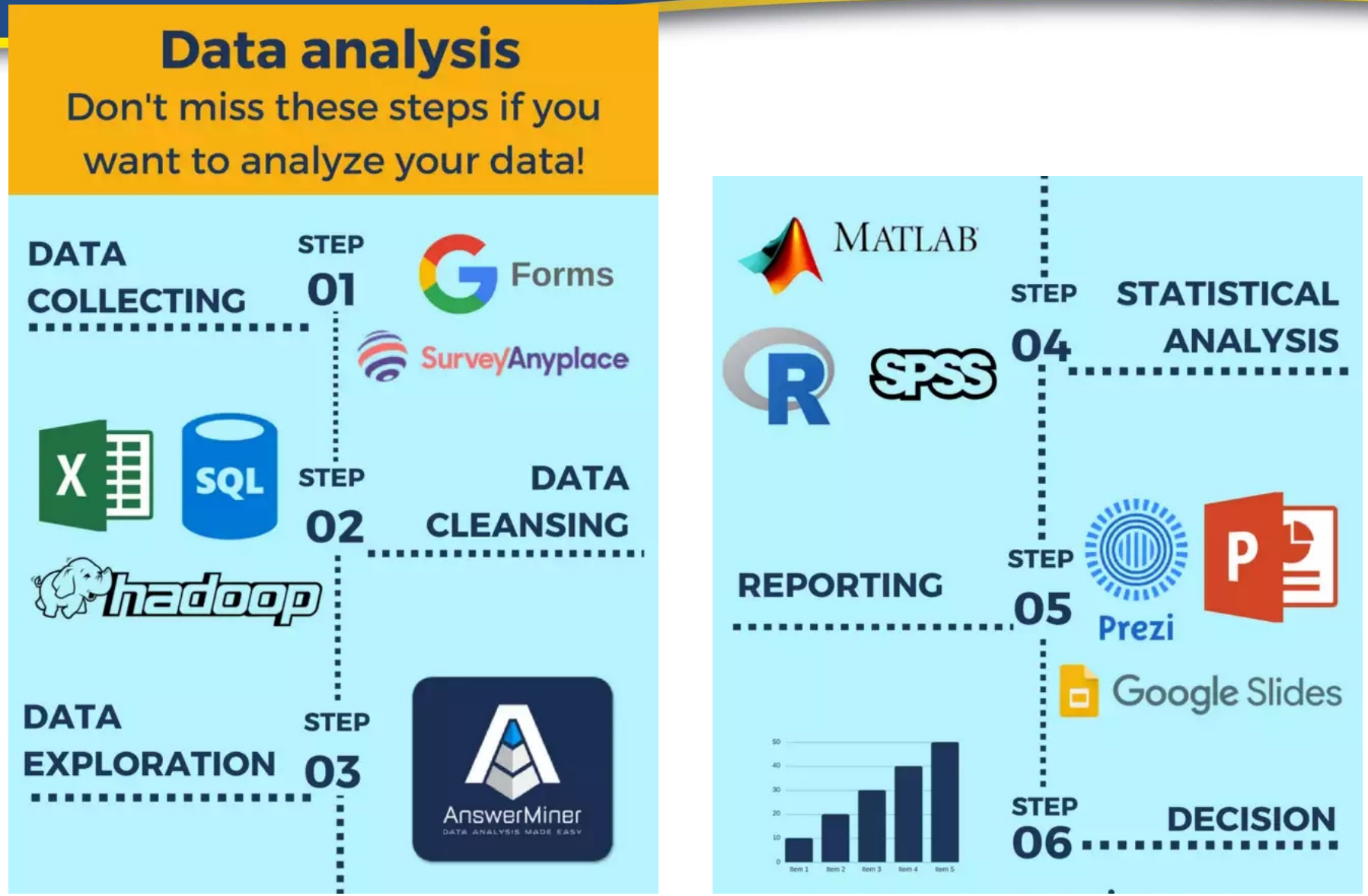
Source: https://hootsuite.com/pages/digital-2020

We are now in the age of Data driven society





Source: US Chamber of Commerce Foundation - https://www.uschamberfoundation.org/blog/post/7-big-facts-about-data-driven-innovation/42045


Data analysis
Don't miss these steps if you want to analyze your data!
DATA COLLECTING
STEP 01
Forms
SurveyAnyplace
STEP 02
DATA CLEANSING
hadoop
DATA EXPLORATION
STEP 03
AnswerMiner
DATA ANALYSIS MADE EASY
MATLAB
STEP 04
STATISTICAL ANALYSIS
SPSS
REPORTING
STEP 05
Prezi
Google Slides
STEP 06
DECISION

RStudio

File Edit Code View Plots Session Build Debug Profile Tools Help

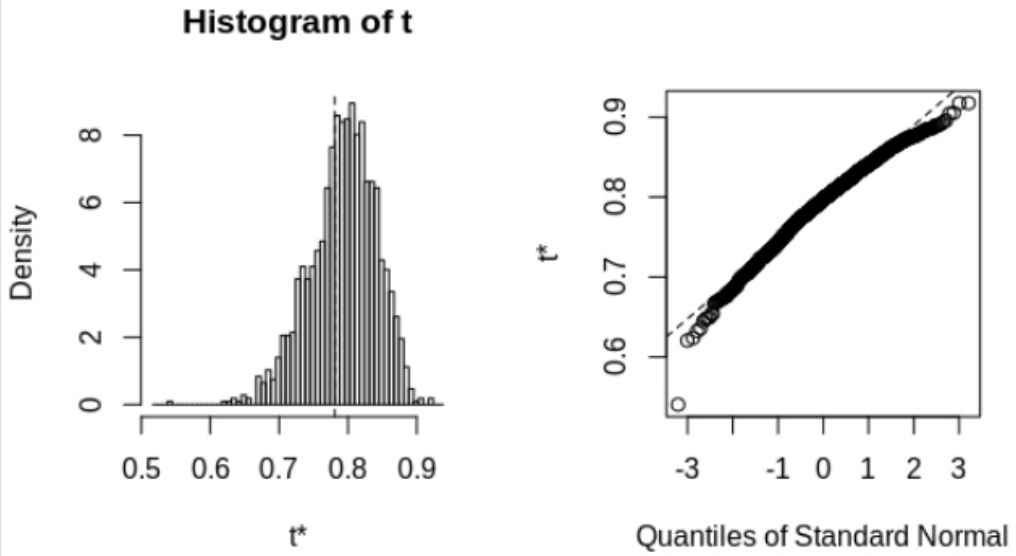
Bootstrapping.R*

```r
# Author DataFlair
library(boot)
# Creating Function to obtain R-Squared from the data
r_squared <- function(formula, data, indices) {
  val <- data[indices,] # selecting sample with boot
  fit <- lm(formula, data=val)
  return(summary(fit)$r.square)
}
# Performing 1500 replications with boot
output <- boot(data=mtcars, statistic=r_squared,
               R=1500, formula=mpg~wt+disp)

# Plotting the output
output
plot(output)

# Obtaining a confidence interval of 95%
boot.ci(output, type="bca")
```

Environment | History | Connections

results	List of 11
Functions	
fc	function (d, i)
r_squared	function (formula, data, indices)

Files | Plots | Packages | Help | Viewer



Source: https://data-flair.training/blogs/bootstrapping-in-r

Typical Business Analytics

Source: https://kwanjaiservices.com/?p=1743

Controversial Uses & Backfire

THE WALL STREET JOURNAL.

Subscribe | Sign In

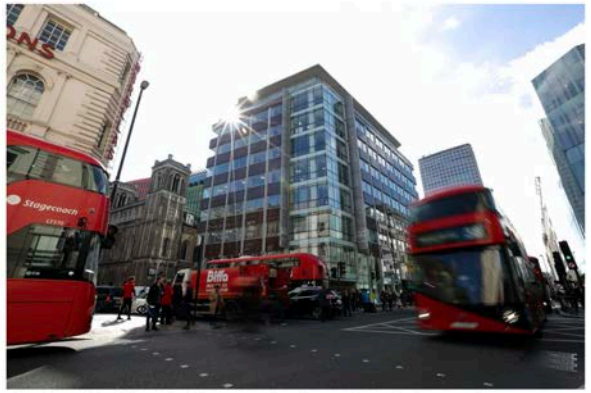
English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business **Tech** Markets Opinion Life & Arts Real Estate WSJ. Magazine

TECH

Cambridge Analytica Revenue Fell as Questions About Data Tactics Surfaced

Under fire from regulators, data-mining company is shutting down



The shared building which houses the offices of Cambridge Analytica in central London, on March 21, 2018.

PHOTO: DANIEL LEAL-OLIVAS/AGENCE FRANCE-PRESSE/GETTY IMAGES

By Peg Brickley
June 1, 2018 3:56 pm ET

PRINT TEXT 1

RECOMMENDED VIDEOS

1. Why Early Voters Are Breaking Records
2. Former Google CEO Sees Antitrust Law as 'Very Blunt Instrument'
3. WSJ/NBC Survey Shows No Swing to Trump Among Wavering Voters
4. Video of Walter Wallace Police Shooting Sparks Protests in Philadelphia
5. Fracking: The Unexpected Issue That Could Determine the 2020 Election

Facebook Seeks Shutdown of NYU Research Project

By Jeff Horwitz October 23, 2020 08:59 pm ET

The company is demanding that a New York University research project cease collecting data about its political-ad-targeting practices, setting up a fight with academics seeking to study the platform without the company's permission.

WSJ PRO PRO CYBER NEWSLETTER

Cyber Daily: U.S. Has Authority to Ban TikTok, Government Lawyers Say | Hackers Extort Therapy Patients in Finland

October 27, 2020 08:36 am ET

The Trump administration said in court papers that Chinese-owned video-sharing app TikTok makes U.S. user data susceptible to influence by Chinese leaders, The Wall Street Journal reports.

WSJ PRO PRO CYBER NEWSLETTER

Cyber Daily: Microsoft Must Increase Protection of French Health Data | Voter database in Georgia County Offline After Ransomware Episode

October 23, 2020 09:03 am ET

A French court has ruled that Microsoft can continue hosting a government-run project aggregating citizens' anonymous health data to use for AI-based research, but must guarantee no data will be sent to the U.S. or be shared with American intelligence authorities. It's the latest move in Europe to assert more control over data movement to the U.S., WSJ Pro's Catherine Stupp reports.

WSJ PRO PRO CYBER NEWSLETTER

Cyber Daily: Security Experts Alarmed Over 'Broken' Cyber Product Market | Voters Report Threatening Email Campaign

October 22, 2020 08:47 am ET

Keeping up with hackers requires cybersecurity vendors to update technology frequently, but this can stymie corporate security chiefs, who often don't have enough information or resources to properly size up products, WSJ Pro's James Rundle reports. Many boards outsource evaluations of cybersecurity preparedness to consultancies to avoid direct culpability when things go wrong, according to one investment chief.

California Probing Facebook's Privacy Practices

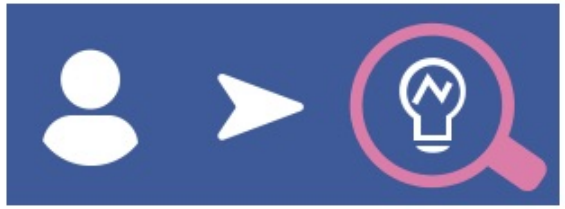
By Sebastian Herrera November 6, 2019 06:31 pm ET

California is investigating Facebook's privacy practices, the state's attorney general revealed in a lawsuit that accuses the tech giant of failing to adequately comply with information requests that the company said it has satisfied.

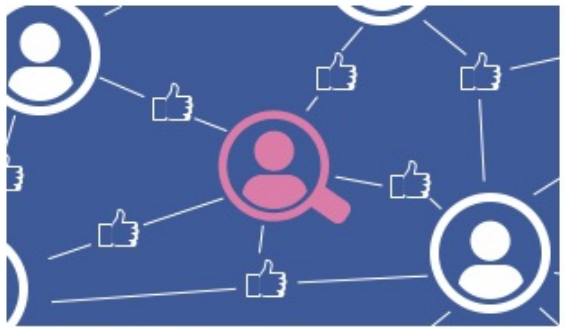
Source: WSJ

How was Facebook users' data misused?

1. In 2014 a Facebook quiz invited users to find out their personality type

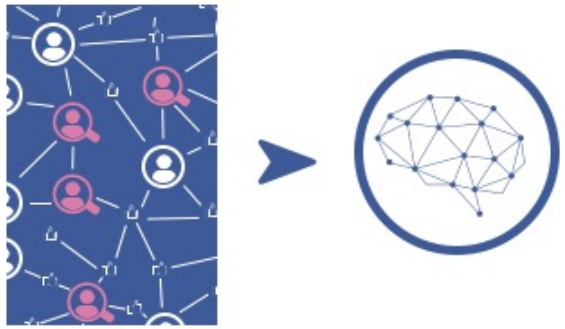


2. The app collected the data of those taking the quiz, but also recorded the public data of their friends

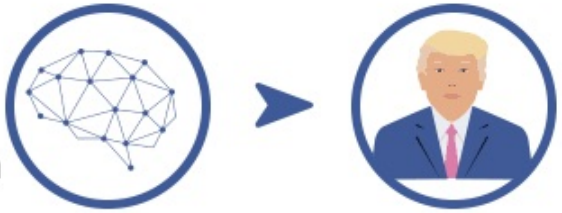


3. About 305,000 people installed the app, but it gathered information on up to 87 million people, according to Facebook

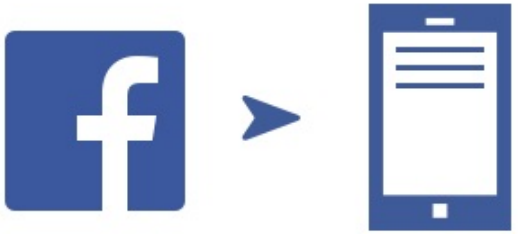
4. It is claimed at least some of the data was sold to Cambridge Analytica (CA) which used it to psychologically profile voters in the US



5. CA denies it broke any laws and says it did not use the data in the US presidential election



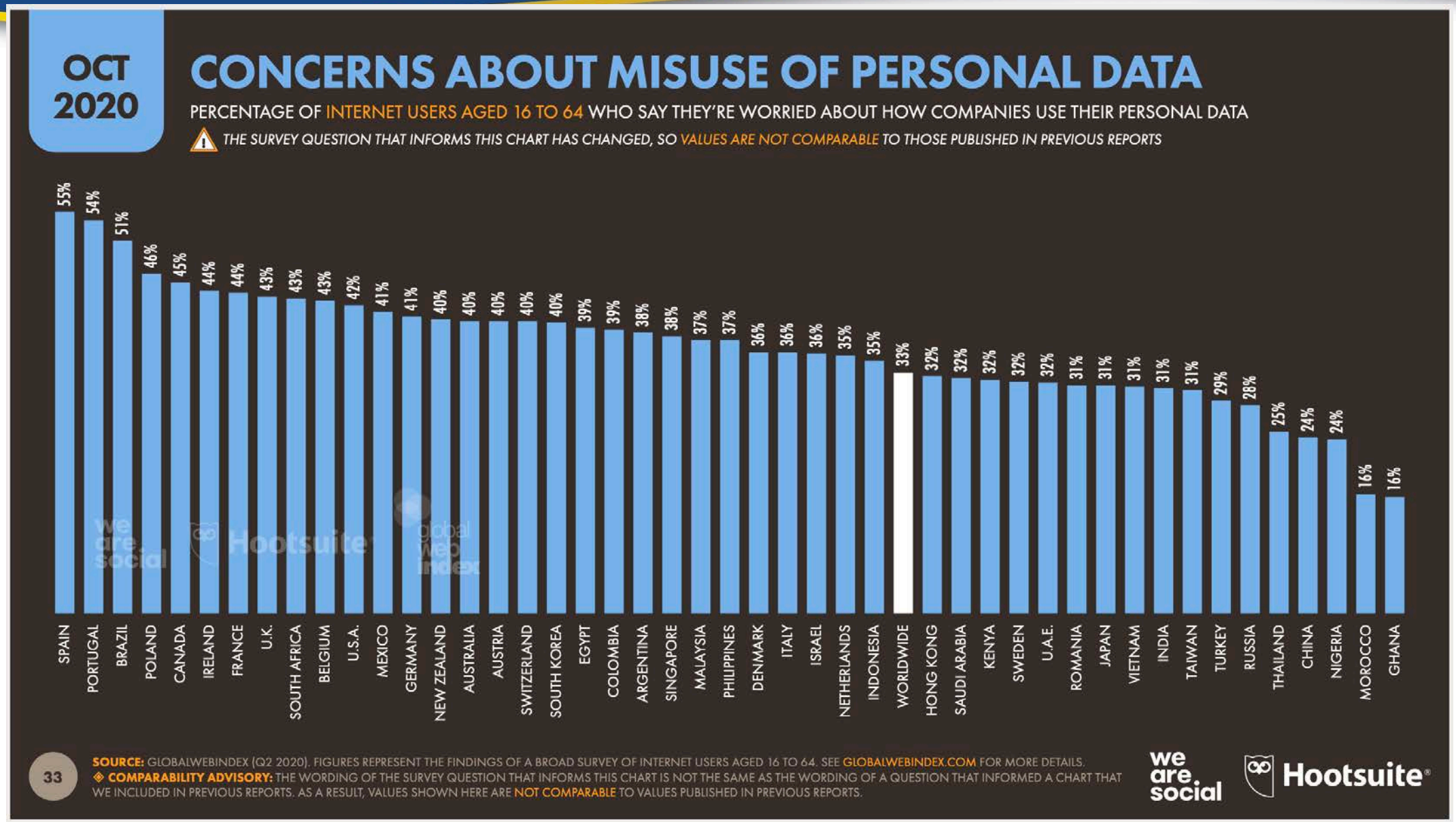
6. Facebook sends notices to users telling them whether their data was breached



CA denies any wrongdoing. Facebook has apologised to users and says a "breach of trust" has occurred.

Source: https://www.bbc.com/news/amp/technology-47281906

Data Governance & Security
Privacy, Legal, Social, Ethics



Source: https://hootsuite.com/pages/digital-2020

What Is Personal Data?

- **Any information that relates to an identified or identifiable living individual**

  Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

- **Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data.**

  For data to be truly anonymized, the anonymization must be irreversible.

Source: European Commission – https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Examples of Data

Personal

- a name and surname
- a home address
- an email address such as `name.surname@company.com`
- an identification card number
- location data, e.g. mobile phone location
- an Internet Protocol (IP) address
- a cookie ID

Personal (cont'd)

- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Non-Personal

- a company registration number
- an email address such as `info@company.com`
- anonymized data.

Source: European Commission – https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Concerns

For Data Owners

- Privacy
- Spams / Annoyance / Unsolicited ads.
- Identity Theft
- Commercial frauds
- Defamation
- Business crimes

For Users of Data

- Ethics
- Legal liabilities

  Fines

  Imprisonment

  for Individuals and Business Entities

Source: European Commission – https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties: fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as

genetic | mental | cultural | economic | social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response. Yes

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data controllers must ensure adequate contracts are in place to **govern data processors**.

Data processors can be held **directly liable** for the security of personal data.

Controllers must have a **legal basis for processing** and collecting personal data.

One-stop shop: international companies will only have to deal with one supervisory data protection authority.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

You have to comply with EU GDPR by MAY 2018

Source: IT Governance Ltd., U.K. – https://www.pinterest.com/pin/521433081677546669

Use Cases

Public Security, Public Health and Smart Cities

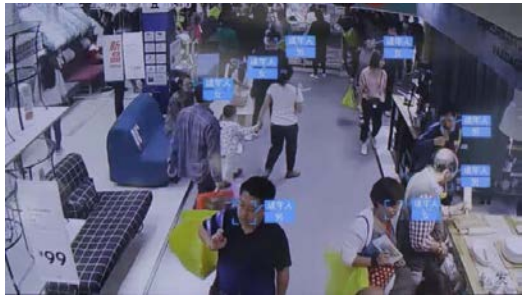
TECH & SCIENCE

China Is Exporting AI Surveillance Technology to Countries Around the World

BY **STEVEN FELDSTEIN** ON 4/23/19 AT 12:18 PM EDT

Visitors are filmed by AI security cameras using facial recognition technology at the 14th China International Exhibition on Public Safety and Security at the China International Exhibition Center in Beijing on October 24, 2018.

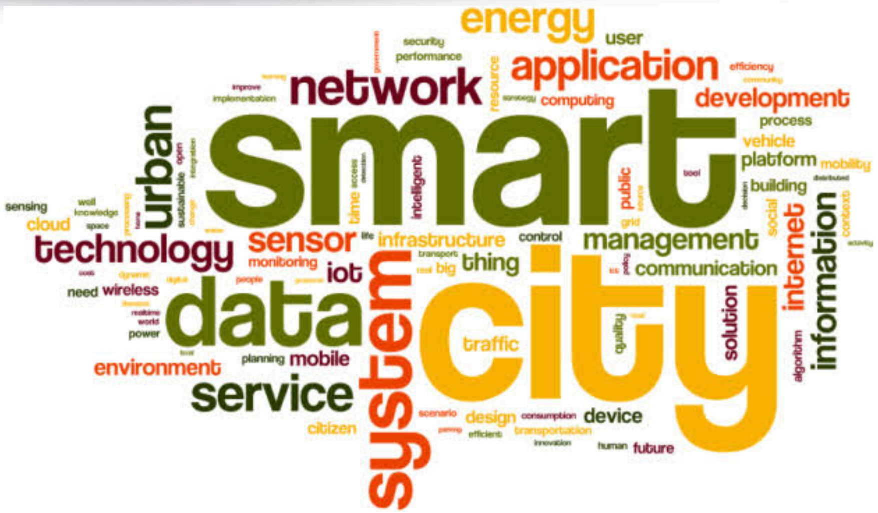
NICOLAS ASFOURI/AFP/GETTY IMAGES

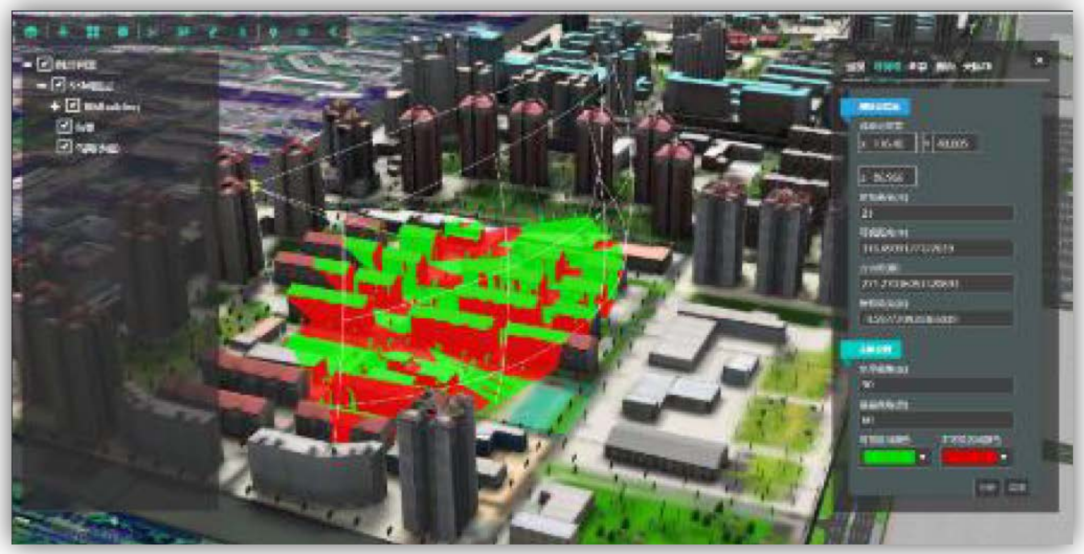


Source: Newsweek; New York Times; Technocracy; SCMP

Covid-19 contact-tracing app : Supervision and surveillance by CCSA

Source: Thailand Center for Covid-19 Situation Administration (CCSA) via The Nation

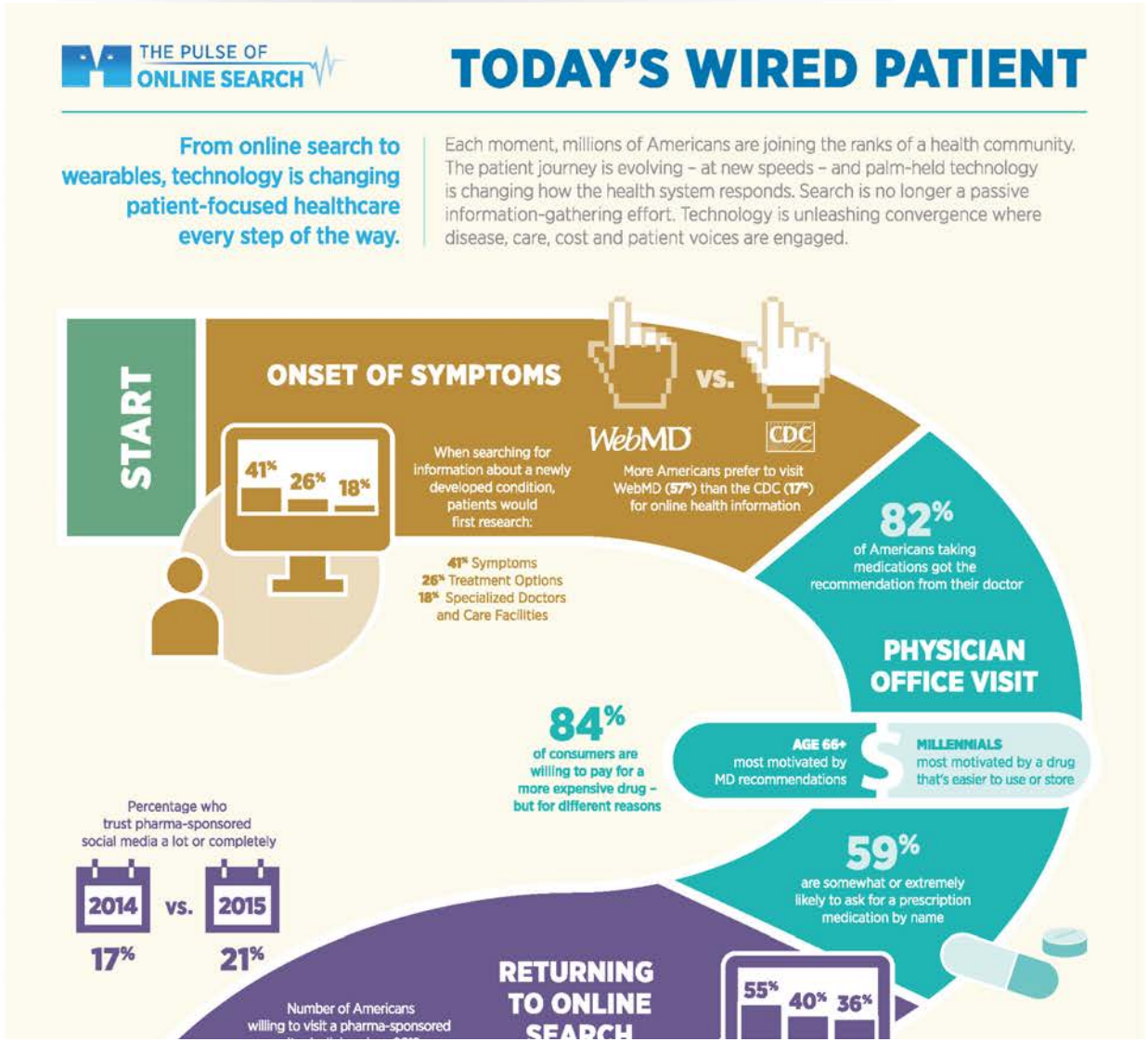


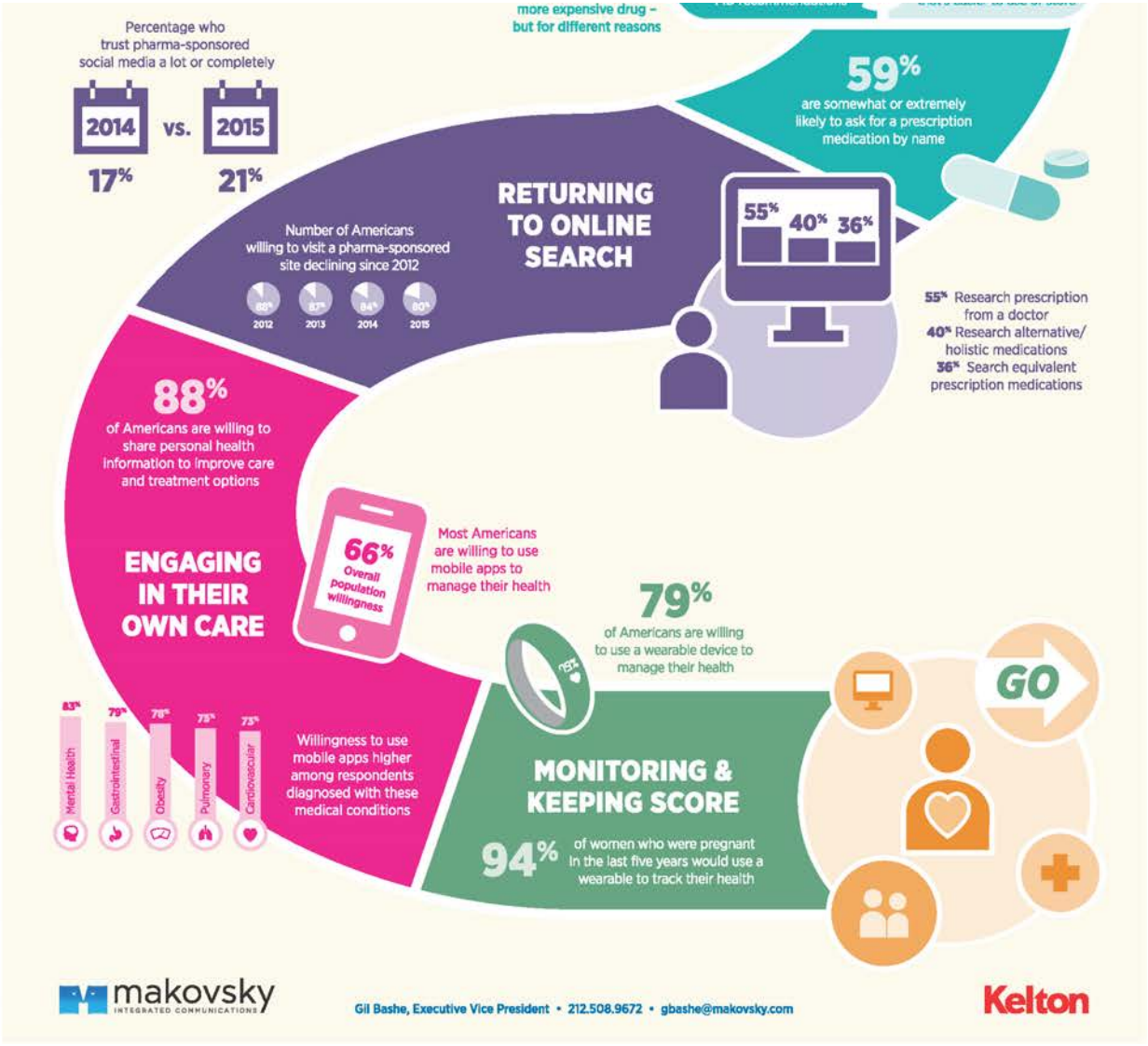


Source: courtesy of SuperMap; ScienceDirect; google images

Sovereign States exert Certain Levels of Privileges over Collection and Processing of Data for Public Benefits

Private Health





Source: https://pin.it/1Iqob7J

THE DIGITAL HOSPITAL: 82 COMPANIES REINVENTING THE PRACTICE OF MEDICINE

CARE PLANNING

dbazahealth, caremerge, caresync, Oncora Medical, Wellframe, rimidi

SUPPLY MANAGEMENT

AETHON, Lab Sensor Solutions

EMR/ PRACTICE MANAGEMENT

Modernizing Medicine, pokitdok, CareCloud, eso, practicefusion, medCPU, FLATIRON, AUGMEDIX, yosko

COMMUNICATION

DrFirst, [m]pirik, cureatr, voalte, BeckonCall, patientsafe, Stitch, tigertext

RADIOLOGY

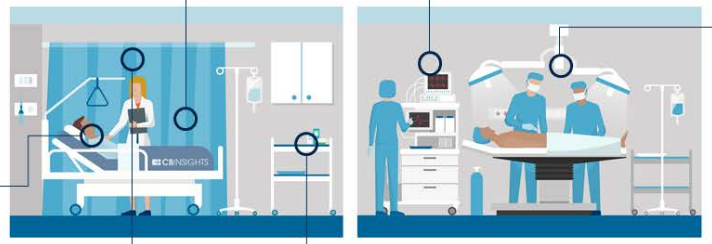
Butterfly Network, Inc., HeartFlow, eagleyemed, ARTERYS, enlitic, lifeIMAGE, SonoCiné, imagia, Trice Medical

DIAGNOSTICS

Genalyte, freenome, BLUEBEE, Lunit, lumiata

PATIENT MONITORING

SENTRIAN, MediBeacon, Glytec, OptiScan, Ornim medical, EarlySense, endotronix



SURGERY

gauss surgical, intellijoint surgical, TOUCHSURGERY, CMR, SURGICAL THEATER, Simulated Surgical Systems, LLC, OrthoSensor

MEDICATION MANAGEMENT

PerceptiMed, TALYST, ZappRx, CAPSULE, RxRevu

REFERRALS

aidin, Arista|MD, GRAND ROUNDS, KYRUUS, SOLERA, Healthify

HOSPITAL NAVIGATION

GOZIO Health, Connexient

READMISSIONS / EMERGENCY DEPARTMENT

Qventus, jvion, Position Health, check-ER

INFECTION CONTROL

AltitudeMedical, XENEX Germ-Zapping Robots, Hyginex, Hand-in-Scan hand hygiene control

PATIENT EXPERIENCE

Bivarus Patient-Centered Analytics, NarrativeDx, medstatix, appliedVR

CARE COORDINATION

HEALTH GORILLA Online Healthcare Marketplace, DASH, HealthLoop, SILVERVUE

CBINSIGHTS

Source: https://www.cbinsights.com/research/digital-health-medicine-market-map-company-list

SECURITY

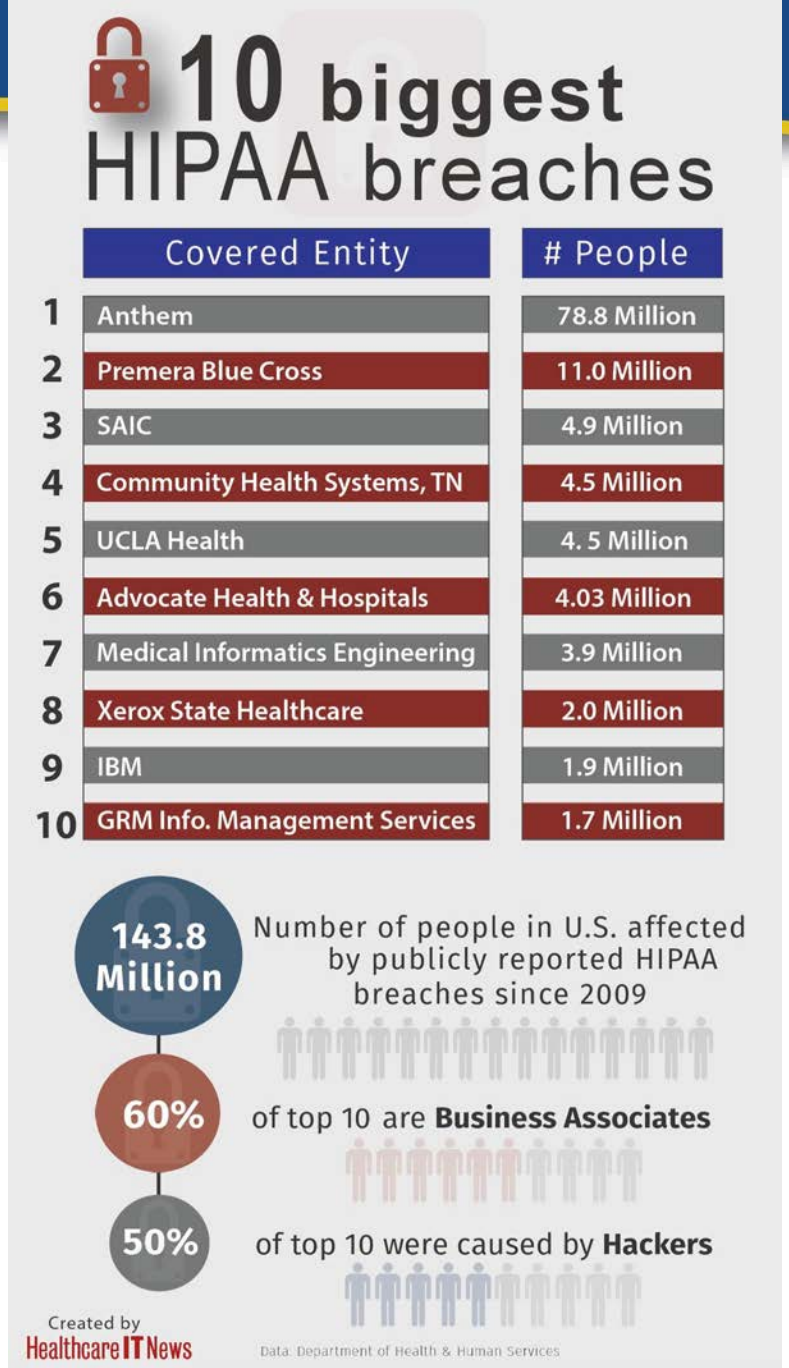
What Happens to Stolen Healthcare Data?

As patients demand increased security for their medical records, healthcare organizations face an uphill challenge to protect the data.

What Threats Are Associated with Stolen Patient Data?

Although stolen health data can be used to carry out a variety of crimes, two scenarios are detrimental: leveraging details specific to a disease or terminal illness, and long-term identity theft.

"Traditional criminals understand the power of coercion and extortion," Kellermann says. "By having healthcare information — specifically, regarding a sexually transmitted disease or terminal illness — that information can be used to extort or coerce someone to do what you want them to do."



TEAM GROUP

HIPAA COMPLIANCE CHECKLIST

TECHNICAL PROTECTIONS

- ENCRYPT & AUTHENTICATE EPHI
- CONTROL/LOG ACCESS & CHANGES TO EPHI
- AUTO-LOGOFF

PHYSICAL PROTECTIONS

- CONTROL/MONITOR PHYSICAL ACCESS
- MANAGE WORKSTATIONS
- PROTECT & TRACK EPHI DEVICES

ADMINISTRATIVE PROTECTIONS

- ASSESS & MANAGE RISK
- TRAIN STAFF
- BUILD/TEST CONTINGENCIES
- BLOCK UNAUTHORIZED ACCESS
- SIGN BAAS
- DOCUMENT SECURITY INCIDENCES

HIPAA PRIVACY RULE TO-DO

- RESPOND TO PATIENT ACCESS REQUESTS
- INFORM PATIENTS WITH NPPS
- TRAIN STAFF
- MAINTAIN EPHI INTEGRITY
- GET PERMISSION TO USE EPHI
- UPDATE FORMS/COPY

HIPAA BREACH NOTIFICATION RULE TO-DO

- PROMPTLY NOTIFY PATIENTS
- HHS & POTENTIALLY THE MEDIA
- ENSURE YOUR NOTIFICATION CONTAINS THE 4 REQUIRED ELEMENTS

HIPAA OMNIBUS RULE TO-DO

- REFRESH YOUR BAA
- SEND NEW COPIES
- UPDATE PRIVACY POLICIES
- MODERNIZE NPPS
- TRAIN STAFF

HIPAA Compliance for Therapists

Email and Texting with Clients

- Employ secure email/text (for ex., Hushmail and Signal)
- Build competence with secure email/text option
- Develop communication policy (boundaries, availability, expected turnaround etc.)

Collecting Payment

- Be careful storing credit card info (use practice management system)
- Most payment systems are fine (if not invoicing/scheduling appoints.)
- Examples: Square and Stripe

Online Therapy

- Learn how to use video (lighting, camera angles, distance)
- Set up environment for clear internet connection (ex. VSee)
- Develop tech failure and client crisis protocols

Record-Keeping

- Only keep electronic records if there is value/requirement
- If you keep records on your computer, fully-encrypt, back-up and fully-encrypt every back-up on every gadget
- Employ strong passwords and anti-malware software

Website

- Post Notice of Privacy Practices (HIPAA form)
- Do not use web host's unsecure email to support "contact me"
- Forms for clients can be downloadable but returned via secure email or system portal

Reference:
Huggins, R. (2017, July 8). HIPAA Compliance: Private Practice Security Tips.

Source: https://pin.it/3qGC9cf - https://pin.it/2HAXrWU

LET DOCTORS BE DOCTORS

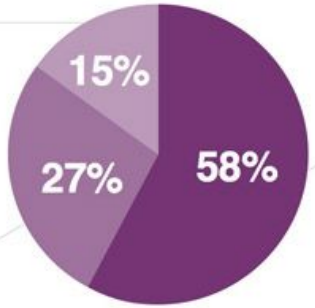
#LetDoctorsBeDoctors is a movement that encourages health care professionals to air frustrations with laggard software (specifically EHRs) and advocate for better technology.

HERE'S WHAT THEY'RE SAYING

6 million people engaged
700+ posts
65,000+ visits
LetDoctorsBeDoctors.com

NURSES AND NURSE PRACTITIONERS
"Help us help patients."

OTHER HEALTH CARE PROVIDERS (HCPs)
"Fill-in-the-blank click lists are soul crushing."



PHYSICIANS
"I mortgaged my future with $200k of debt to learn to care for humans, not computers."

TOP 4 WAYS EHRS HURT

We asked health care professionals how EHRs get in their way.*

TREATING COMPUTER SCREENS, NOT PATIENTS

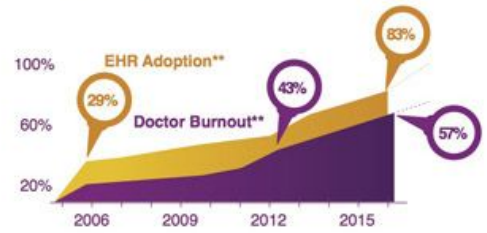
#1 frustration for doctors is the time spent in front of an EHR screen

53% of HCPs concerned about EHR distraction also said EHRs prevent quality care.

"Sad to spend my day staring at a screen while people share vulnerable moments."
MD from California

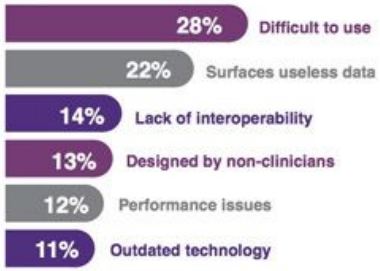
PROVIDER BURNOUT

1 out of 5 providers said EHRs prevent them from doing what they trained for—and they're ready to call it quits.



FAILING TECHNOLOGY

Top ways EHR technology fails



WASTING TIME ON DOCUMENTATION

#1 frustration for RNs is the time spent charting

80% of HCPs cited excessive time spent on admin tasks and after-hour charting.

"It shouldn't take us an hour to document 10 minutes of care."
RN from Texas

Source: https://pin.it/5P3Fdto

Implications for

Data Engineers & Data Scientists

GDPR Compliance Requirements

4. Accuracy

You must keep the data current, accurate and up to date.

3. Storage Limitation

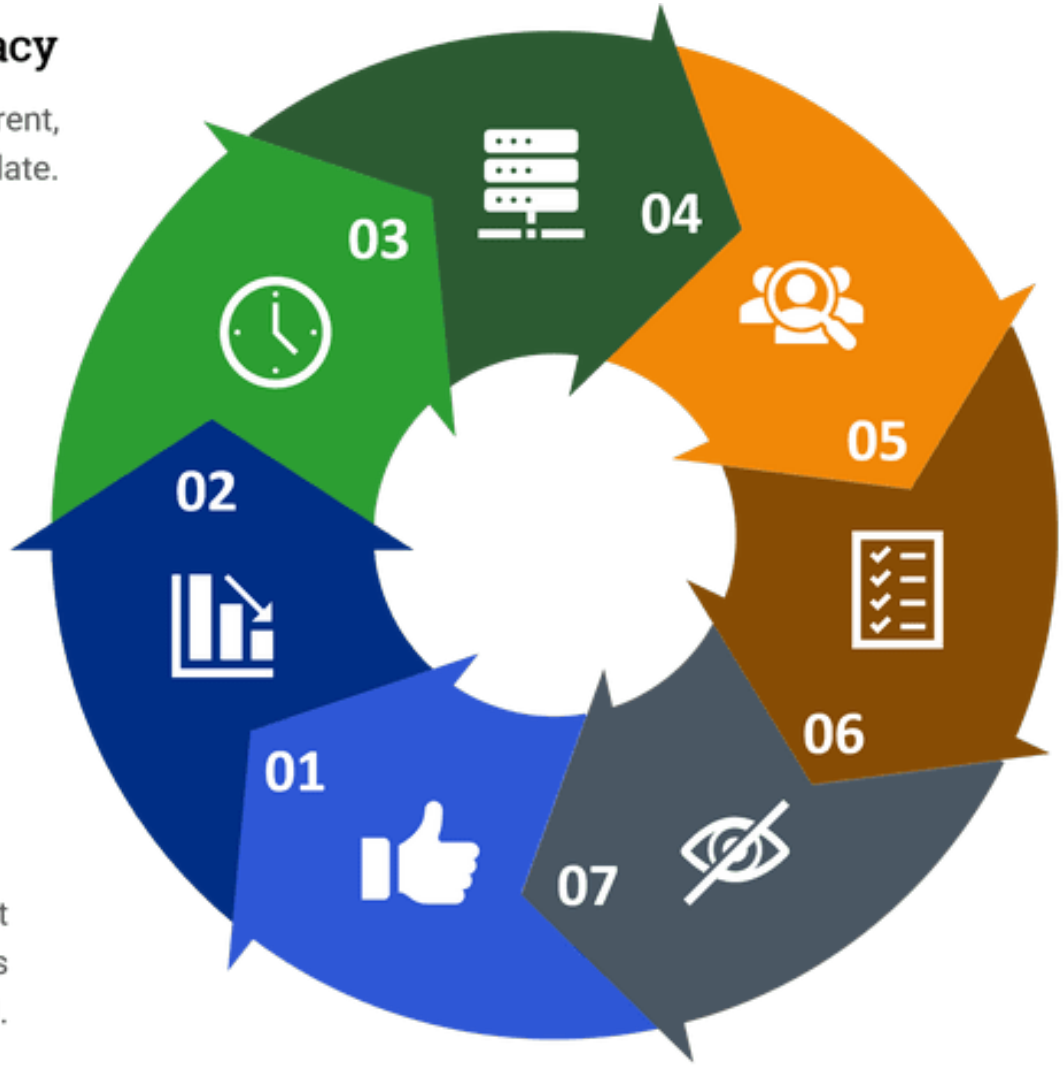
You may only store personally identifying data for as long as necessary for the specified purpose.

2. Data Minimization

You should collect and process only as much data as absolutely necessary for the purposes specified.

1. Accountability

Documentation and personnel must reflect the best practices established.



5. Lawfulness, fairness & transparency

Must have a lawful basis to use the data and consent from the client while keeping their individual rights in mind.

6. Purpose Limitation

You must process data for the legitimate purposes specified explicitly to the client when you collect it.

7. Integrity & Confidentiality

You must do your due diligence to maintain confidentiality, integrity and availability of data. This includes:

- Risk Assessments
- Implement Policies and Procedures
- Train Employees

Source: Third Rock, Inc. – https://thirdrock.com/gdpr

TEAM GROUP

Do's

- Shred personal data if in paper form.
- Arrange certified confidential waste disposal for large amounts of personal data.
- Keep your usernames and passwords secure.
- Dispose of personal data promptly.
- Report any data breaches immediately.
- Undertake regular training on GDPR.
- Be vigilant with emails and attachments.
- Familiarise yourself with your organisation's documentation and policies.
- Log out when not using a digital service.
- Only use personal data if you need to, and for as long as you need it.
- Audit the data you are using on a day to day basis within the scope of GDPR.
- Verify an individual before handing over personal data.

Don'ts

- Leave any personal information lying around.
- Give your username or password to anyone.
- Dispose of personal data in regular bins or recycling if it has not been shredded or destroyed.
- Open emails or attachments from unknown sources.
- Duplicate personal data unnecessarily e.g. printing it out.
- Download business data onto personal devices unless authorised.
- Leave your computer logged in if you can access personal data from it.
- Store your passwords in browsers.
- Log on to public Wi-Fi or unsecured networks whilst working with personal data.
- Provide access to personal data unless it is necessary and lawful.

The Data Protection Officer (DPO) or relevant individual in your organisation will be able to direct you to the necessary documentation and is the first port of call for any concerns you may have.

Name of DPO or relevant individual:

Source: https://pin.it/4Y8fe9X

Final Remarks on

Governance: The Big Picture

What is Corporate Governance?

- Corporate governance is the system of **rules, practices, and processes** by which a firm is directed and controlled.
- Corporate governance essentially involves **balancing the interests** of a company's many **stakeholders**, such as shareholders, senior management executives, customers, suppliers, financiers, the government, and the community.
- Since corporate governance also provides the framework for attaining a company's objectives, it encompasses practically **every sphere of management**, from action plans and internal controls to performance measurement and corporate disclosure.

Source: https://www.investopedia.com/terms/c/corporategovernance.asp

Data Governance

Data governance therefore

- is the system of **rules, practices, and processes** by which data within a firm is directed and controlled;
- involves **balancing the interests** of a company's many **stakeholders**;
- encompasses **every sphere of management** within a company.

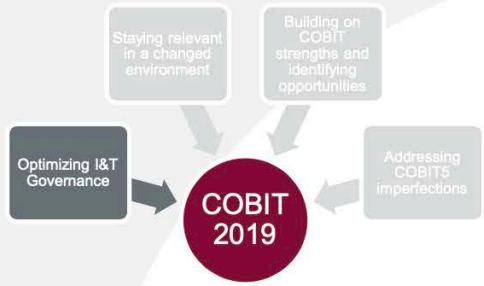
Source: adapted from https://www.investopedia.com/terms/c/corporategovernance.asp

Data Governance …

from IT to I&T

COBIT 2019

OPTIMIZING I&T GOVERNANCE



Enterprise Governance of I&T

Business/IT Alignment

Value Creation

IT - used to refer to the organizational department with main responsibility for technology – versus **I&T** – all the information the enterprise generates, processes and uses to achieve its goals, as well as the technology to support that throughout the enterprise.

COBIT 2019

OVERVIEW
EXTERNAL STAKEHOLDERS

Determines whether the enterprise is compliant with applicable rules and regulations and advises that the enterprise has the right governance system in place to manage and sustain compliance

IT vendor's operations must establish that they are secure, reliable and compliant with applicable rules and regulations

Confirm that a business partner's operations are secure, reliable and compliant with applicable rules and regulations

COBIT 2019

OVERVIEW
INTERNAL STAKEHOLDERS

Provides insights on how to get value from the use of I&T and explains relevant board responsibilities

Provides guidance on how to organize and monitor performance of I&T across the enterprise

Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for strategic opportunities

Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.

Helps manage dependencies on external service providers, provides assurance over IT, and ensures the existence of an effective and efficient system of internal controls

Helps to ensure the identification and management of all IT-related risk

COBIT 2019

KEY CONCEPTS

COMPONENTS OF A GOVERNANCE SYSTEM

- Each enterprise's governance system is built from a number of components
- Components can be of different types
- Components interact with each other, resulting in a holistic governance system for I&T
- These were known as enablers in COBIT 5

Reference: COBIT® 2019 Framework: Basic Concepts: Governance Systems and Components, Figure 4.3

COBIT 2019

Key Takeaways

- Tremendous amount of data are generated, consumed and leveraged for great benefits of Individuals, Businesses and Public nowadays. The growth is exponential.
- With great power comes great responsibility
- Collect, store and process data for a reason
- Handle ‘magic swords’ with care. Always observe good governance principles.
- For managers, plan and manage data across life-cycle properly.
  For operators, act responsibly. Respect owners of data.
- Don’t let privileges become liabilities.

Thank You