African Journal of Engineering & Technology AJET

Article title: Data Privacy: An Overview

Authors: Anour Dafaalla[1]
Affiliations: Sudanese Researchers Foundation, Khartoum, Sudan[1]
Orcid ids: 0000-0003-0654-3615[1]
Contact e-mail: anwarking@gmail.com

License information: This work has been published open access under Creative Commons Attribution License http://creativecommons.org/licenses/by/4.0/, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. Conditions, terms of use and publishing policy can be found at https://www.scienceopen.com/.

Preprint statement: This article is a preprint and has not been peer-reviewed, under consideration and submitted to AJET Blinded Peer Review Platform for open peer review.
Funder: N/A
DOI: 10.14293/S2199-1006.1.SOR-.PPWLERO.v1
Preprint first posted online: 23 November 2020
Keywords: Privacy, Data Protection, Cybersecurity

Data Privacy: An Overview

Dr. Anwar Dafa-Alla, Computer Science Assistant Professor
Sudanese Researchers Foundation
AnwarKing @ Gmail.com

Privacy definition

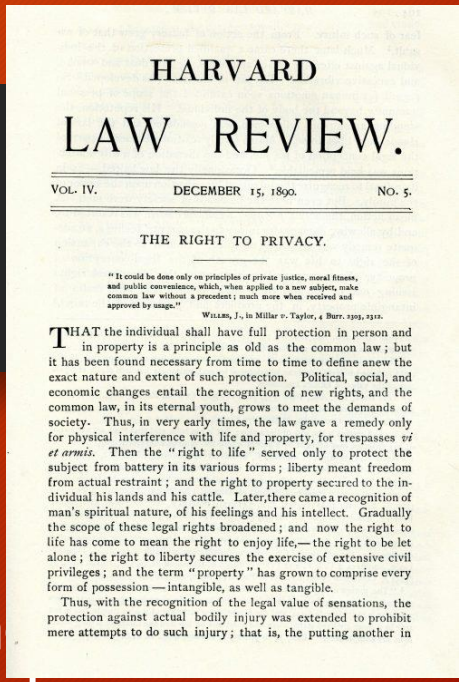
- Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.

- الخصوصية هي قدرة الفرد أو المجموعة على عزل أنفسهم أو الحصول على معلومات عن أنفسهم، وبالتالي التعبير عن أنفسهم بشكل انتقائي.
- مصطلح الخصوصية، في الأصل هو مفهوم يشير إلى نطاق الحياة الخاصة، في العقود الأخيرة تطور على نطاق أوسع، ليضمن الحق في السيطرة على البيانات الشخصية.
-

الخصوصية في الاسلام

- قال الله -عز وجل- في كتابه الكريم: **{يا أيها الذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها}**سورة النور.
- وقال سبحانه: **{ولا تجسسوا ولا يغتب بعضكم بعضا}**سورة الحجرات.
- وقال الرسول صلى الله عليه وسلم: **((من اطلع في بيتِ قومٍ بغير إذنهم فقد حلَّ لهم أن يفقأوا عينه، فإن فقأوا عينه فلا دية له ولا قصاص))**رواه النسائي وصححه الألباني، ورواه مسلم مختصرا.
- وقال صلى الله عليه وسلم: **((من تسَّمع حديث قومٍ وهم له كارهون، صُب في أُذنيه الآنك))**رواه أحمد

History of Privacy



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

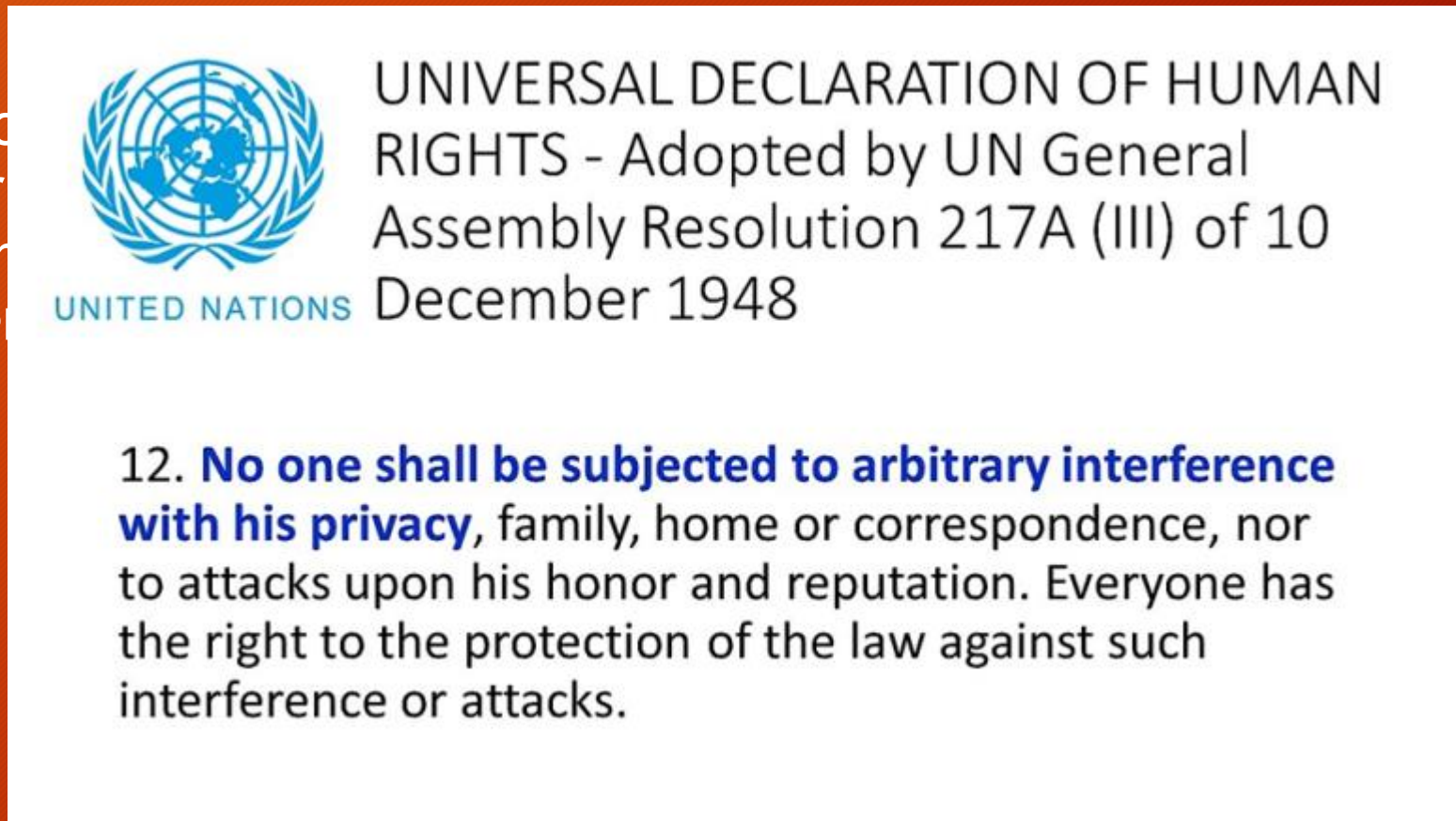
Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

- "**The Right to have privacy**" (4 Harvard L.R. 193 (Dec. 15, 1890)) is a law review article written by Samuel Warren and Louis Brandeis, and published in the 1890 *Harvard Law Review*. It is "one of the most influential essays in the history of American law"[1] and is widely regarded as the first publication in the United States to advocate a right to privacy,[2] articulating that right primarily as a "right to be let alone".

History of Privacy

Article 12.

- No one shall be subjected to
  privacy, family, home or cor
  honour and reputation. Ever
  the law against such interfe



Ideas around privacy

- **Secret**: Ability of someone to control the personal data gathering and usage. One school of thoughts toward being suspicious about hiding, the other being that it is part of individual freedom rights.
- **Calmness**: Possibility for someone to not be disturbed in the daily life, with a control on the ability of people accessing you. It includes the seek for being forgotten.
- **Individual autonomy**: Ability to take important decisions in a way that enable self expression and diverse intimate relationships

Why is Privacy Important?

- To earn and keep public trust

  If the public no longer trusts institutions to protect their PII, public support for these institutions may erode.

- To prevent privacy incidents

  Incidents reported in USA news erode the public's trust in those agencies and are expensive to mitigate. Recovery cost per data breach incident averages $3.6M according to IBM

- To prevent identity theft

  Privacy incidents that raise the risk of identity theft can be lengthy, costly, and stressful to recover from for the individual and institutions.

- It's the law now!

  Failure to follow these laws may result in civil or criminal penalties, or loss of employment.

Personally Identifiable Information (PII)

- PII is information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- Sensitive Personally Identifiable Information (Sensitive PII or SPII) is a subset of PII which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

- Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

Sensitive PII

- The following PII is always *(de facto)* sensitive, with or without any associated personal information, and cannot be treated as low confidentiality:
  - Social Security number (SSN)
  - Passport number
  - Driver's license number
  - Vehicle Identification Number (VIN)
  - Biometrics, such as finger or iris print, and DNA
  - Financial account number such as credit card or bank account number
  - The combination of any individual identifier and date of birth, or mother's maiden name, or last four of an individual's SSN

- The following information is Sensitive PII when associated with an individual:
  - Account passwords
  - Criminal history
  - Ethnic or religious affiliation
  - Last 4 digits of SSN
  - Mother's maiden name
  - Medical Information
  - Sexual orientation

Sensitive PII (continued)

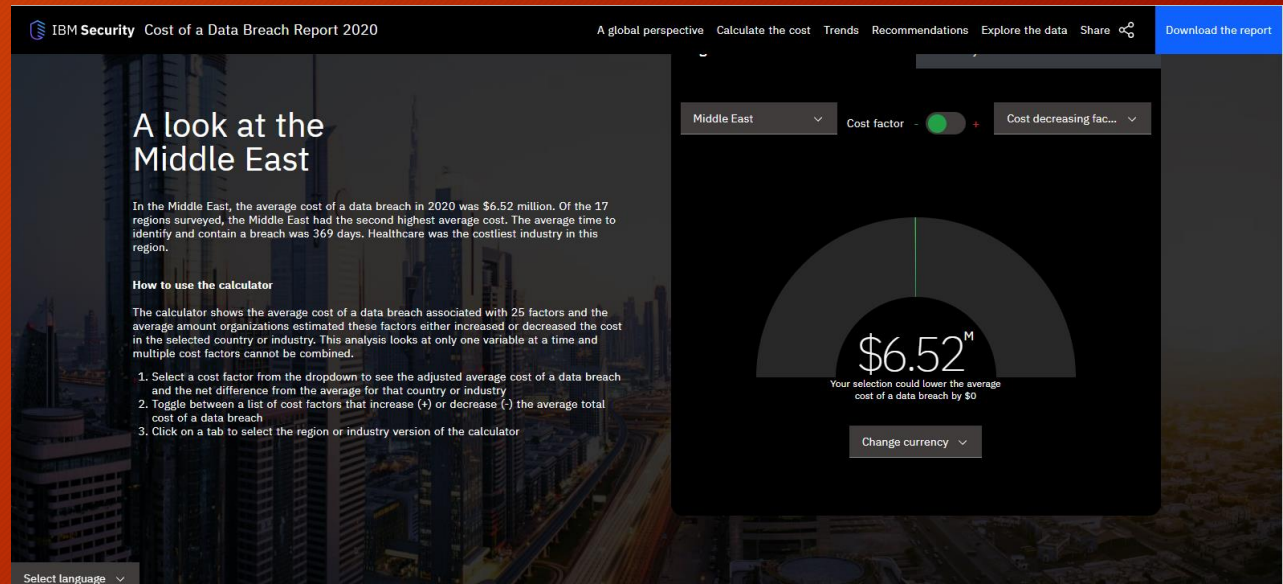
- In addition to *de facto* Sensitive PII, some PII may be deemed sensitive based on context. For example, a list of employee names is not Sensitive PII; however, a list of employees' names and their performance rating would be considered Sensitive PII.

- The following PII is not sensitive alone or in combination unless documented with sensitive qualifying information and may be treated as low confidentiality:
  - Name
  - Professional or personal contact information including email, physical address, phone number and fax number

- Federal employee name, work contact information, grade, salary and position are considered PII. Except for limited circumstances, this information is publically available and is not considered sensitive.

Cost of a Data Breach (IBM)

- Average total cost of a data breach **USD 3.86 million**
- Most expensive country: USD 8.64 million **United States**
- Most expensive industry: USD 7.13 million **Healthcare**
- Average time to identify and contain a breach **280 days**



Privacy types

- Financial privacy, privacy relating to the banking and financial industries
- Information privacy, protection of data and information
- Internet privacy, the ability to control what information one reveals about oneself over the Internet and to control who can access that information
- Medical privacy, protection of a patient's medical information
- Political privacy, the right to secrecy when voting or casting a ballot

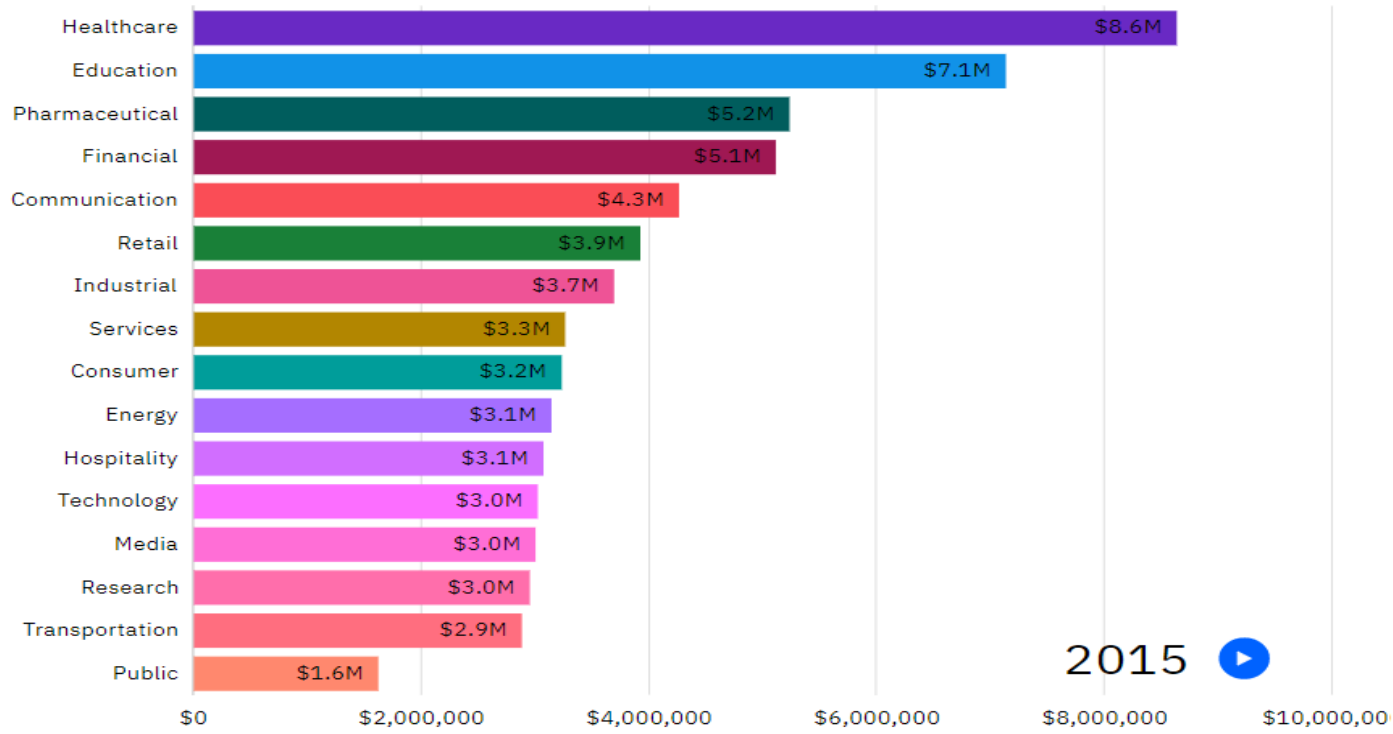
Industry data breach costs have changed over time

Industry trends

Industry data breach costs have changed over time

The average cost of a data breach has fluctuated between $3.50 million and $4.00 million in recent years. But that's not the whole story, as the cost of a breach varies significantly based on industry. Click Play for an animated view of how the average data breach costs in 16 industries have changed over the last six years.

US Dollar



Select language

The 15 biggest data breaches of the 21st century

All bigger than 100 million user's record

1. Adobe
2. Adult Friend Finder
3. Canva
4. Dubsmash
5. eBay
6. Equifax
7. Heartland Payment Systems
8. LinkedIn
9. Marriott International
10. My Fitness Pal
11. MySpace
12. NetEase
13. Sina Weibo
14. Yahoo
15. Zynga

Date: 2013-14
Impact: 3 billion user accounts
Details: Yahoo announced in September 2016 that in 2014 it had been the victim of what would be the biggest data breach in history. The attackers, which the company believed we "state-sponsored actors," compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised passwords were hashed.
Then in December 2016, Yahoo disclosed another breach from 2013 by a different attacker that compromised the names, dates of birth, email addresses and passwords, and security questions and answers of 1 billion user accounts. Yahoo revised that estimate in October 2017 to include all of its 3 billion user accounts.
The timing of the original breach announcement was bad, as Yahoo was in the process of being acquired by Verizon, which eventually paid $4.48 billion for Yahoo's core internet business. **The breaches knocked an estimated $350 million off the value of the company.**

Web Technologies with implication on Privacy

- A few technologies already exist with strong implications on Web Tracking and user Privacy.
- cookies
- HTTP logs
- localStorage
- Do Not Track HTTP Headers
- P3P
- Fingerprinting
- Face recognition

Web Tec10 Types of Data Your Browser Is Collecting About You Right Now

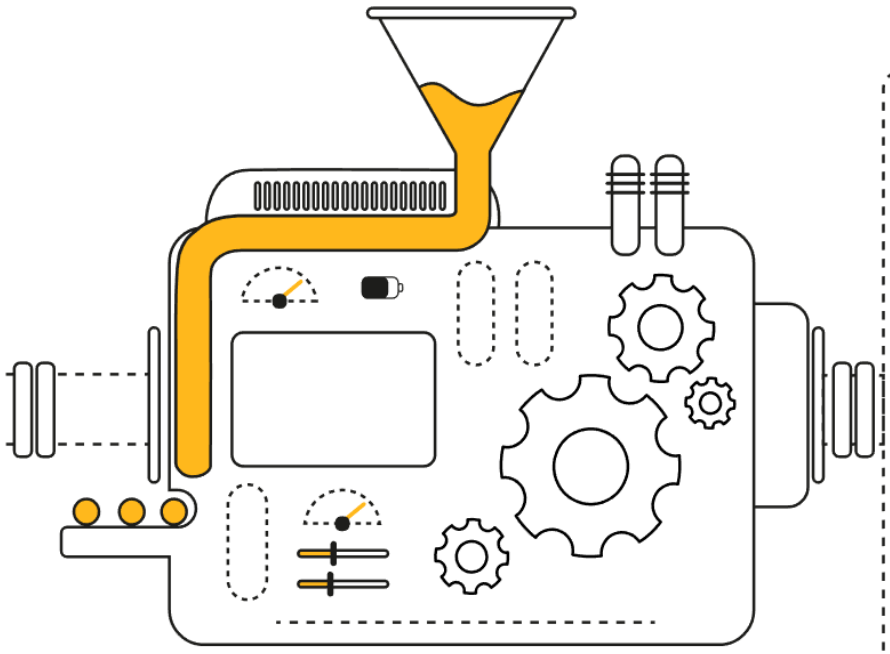
1. Hardware And Software
2. Connection Information
3. Geolocation
4. Browsing History
5. Mouse Movements
6. Your Device's Orientation
7. Social Media Logins
8. Fonts And Language
9. Image Data
10. Technical Information

Browser Extensions Also Collect Data

Check it yourself: https://webkay.robinlinus.com/ https://firstpartysimulator.org/

Digital footprints

- Facebook LikeIDs
- Facebook statuses
- Tweets
- Browsing data
- Open text
- And more...



Individual **profiles**

Psychographics

- BIG5 Personality
- Intelligence
- Life Satisfaction
- Political Views
- Religious Views
- Sexuality
- Profession

Demographics

- Age
- Gender
- Relationship status

Image privacy & the Selfie culture!

- **Exchangeable image file format** (officially **Exif**, according to JEIDA/JEITA/CIPA specifications) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras.

Image privacy & the Selfie culture!

- The following table shows Exif data for a photo made with a typical digital camera.

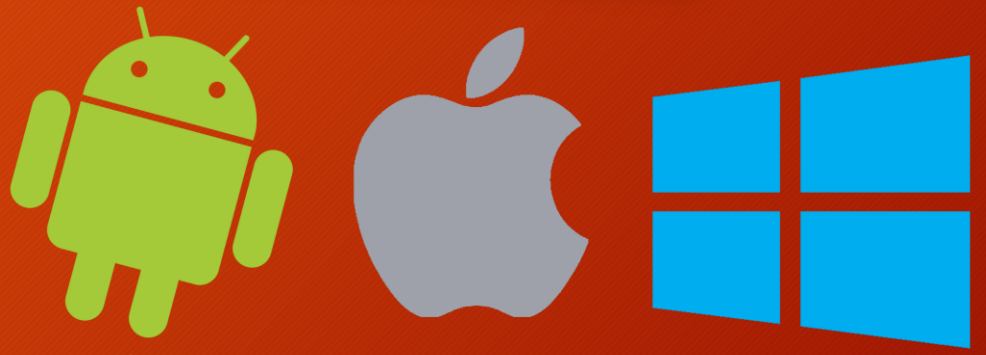
Global Positioning System	
GPS Altitude	31.9 m
GPS Latitude	6deg 14' 7.620"
GPS Longitude	106deg 49' 30.210"
Image Information	
Date and Time	2018:08:24 15:47:27
Manufacturer	Apple
Model	iPhone 6s
Photograph Information	
Aperture	F2.2
Exposure Bias	0 EV
Exposure Mode	Auto
Exposure Program	Auto
Exposure Time	1/874 s
Flash	No, auto
FNumber	F2.2
Focal Length	4.2 mm
ISO Speed Ratings	25
Metering Mode	Multi-segment
Shutter speed	1/874 s
White Balance	Auto

Famous case of Exif

- In December 2012, anti-virus businessman John McAfee was arrested in Guatemala while fleeing from alleged persecution[17] in neighboring Belize. *Vice* magazine had published an exclusive interview on their website with McAfee "on the run"[18] that included a photo of McAfee with a *Vice* reporter taken with a phone that had geotagged the image.[19] The photo's metadata included GPS coordinates locating McAfee in Guatemala, and he was captured two days later.[20] McAfee later claimed to have edited the EXIF data from his phone to provide a false location.[21]

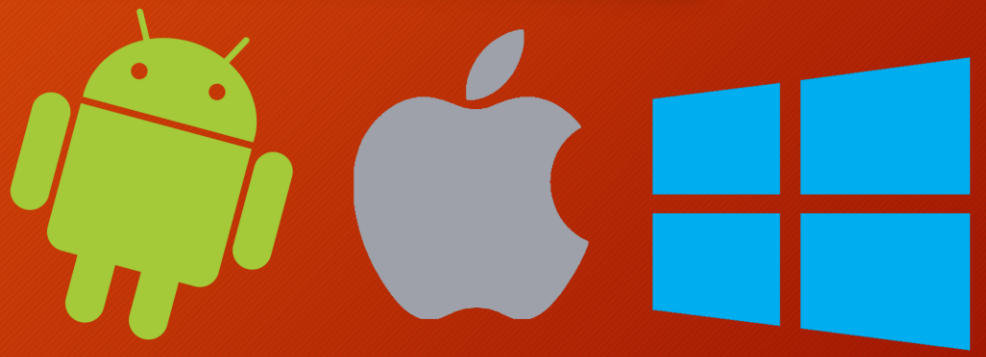
Dealing with user privacy in mobile apps: issues and mitigation

- Mobile phone platforms:
  - usability,
  - flexibility,
  - and low cost



- Became sources and repositories of sensitive information:
- from running performances to positioning data, from travel information to friendship preferences, from personal photos to financial data, etc…

Dealing with user privacy in mobile apps: issues and mitigation



- Most cyber-crime start with personal data stolen, collected on the fly in the network or from databases and applications running on any kinds of platforms.

Mobile Apps

Mohammed Aldoub محمد الدوب
@Voulnet

احذر من برنامج Muslim Pro للقرآن والقبلة والأذان!

هذا التطبيق خان المستخدمين،المسلمون بطبيعة الحال، وقام ببيع بياناتهم ومن بينها بيانات الموقع الجغرافي لجهات مثل الجيش الأمريكي والحكومة الأمريكية وغيرها!

هذا التطبيق له قرابة 100 مليون عملية تحميل!

مصدر:

vice.com/amp/en/article...
pic.twitter.com/iRhsItq6ID

Translate Tweet

11:07 PM · 16 Nov 20 · Twitter for Android

174 Retweets **14** Quote Tweets **164** Likes

VICE

MOTHERBOARD
TECH BY VICE

How the U.S. Military Buys Location Data from Ordinary Apps

A Muslim prayer app with over 98 million downloads is one of the apps connected to a wide-ranging supply chain that sends ordinary people's personal data to brokers, contractors, and the military.

By Joseph Cox

Nov 16 2020, 3:35pm Share Tweet Snap

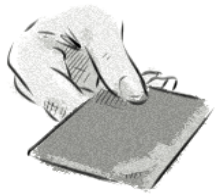
Data Brokers

Credit: Pixabay

- Data brokers (aka information brokers, data providers, and data suppliers) are companies that collect data themselves or buy it from other companies (like a credit card company), crawl the internet for useful information about users – legally or otherwise – and aggregate that information with data from other sources (e.g. offline sources). Most people are not even aware such companies exist, but data brokerage has become a lucrative industry that generates $200 billion in revenue yearly, and it's still growing.
- **Data Brokers: A Weak Link in National Security** Banning TikTok and other Chinese apps won't solve a thing if China can simply buy the data it wants from private brokers.

Free to play games and apps

Registered loyalty cards



Purchase history

Data from public social media profiles

Publicly available information

Data broker

Other data brokers

People with depression and substance abuse

People who recently got married

People who donate to international aid charities

Compulsive buyers

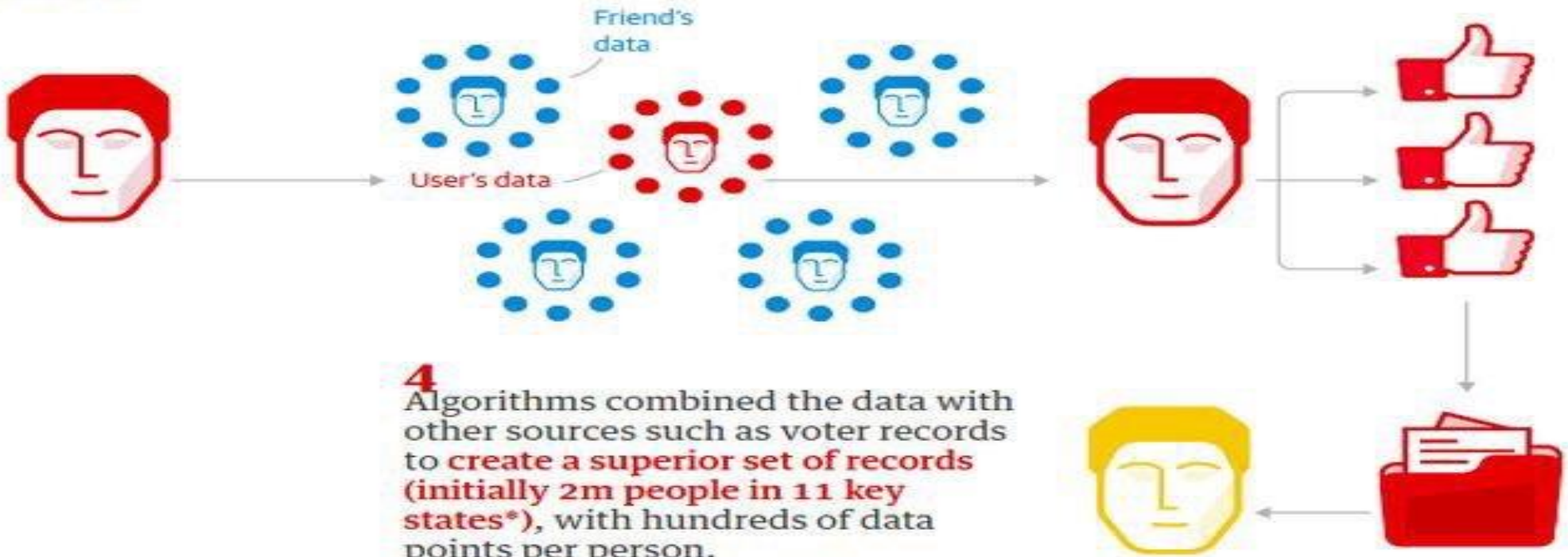
Expectant parents

Cambridge Analytica: how 50m Facebook records were hijacked

1
Approx. 32,000 US voters ('seeders') were **paid $2-5 to take a detailed personality/ political test** that required them to log in with their Facebook account

2
The app also **collected data such as likes and personal information** from the test-taker's Facebook account, as well their **friends'** data, amounting to over 50m people's raw Facebook data

3
The **personality quiz results** were paired with their Facebook data – such as **likes** – to seek out psychological patterns



4
Algorithms combined the data with other sources such as voter records to **create a superior set of records (initially 2m people in 11 key states*)**, with hundreds of data points per person.
These individuals could then be targeted with **highly personalised advertising** based on their personality data

Guardian graphic. *Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, West Virginia

VOTING AND REGISTRATION

Data Tables

Datasets

Data Tools

< Back to Data

Datasets

In addition to the Voting and Registration estimates made available on this website, data users can obtain Public Use Microdata Files for elections that the U.S. Census Bureau has data for via DataFerrett, the Bureau's online data access application. The November CPS data files, and entire datasets, are accessible for free through the DataFerrett tool dating back to 1994. The CPS FTP site is another location for obtaining voting and registration data.

Data users can also obtain CPS Voting and Registration data files from non-governmental websites. The National Bureau of Economic Research website contains voting supplement datasets starting in 1994. The IPUMS-CPS website maintained by the University of Minnesota includes voting supplement datasets starting in 1976."

Sign Up for Email Updates

To sign up for updates please enter your contact information below.

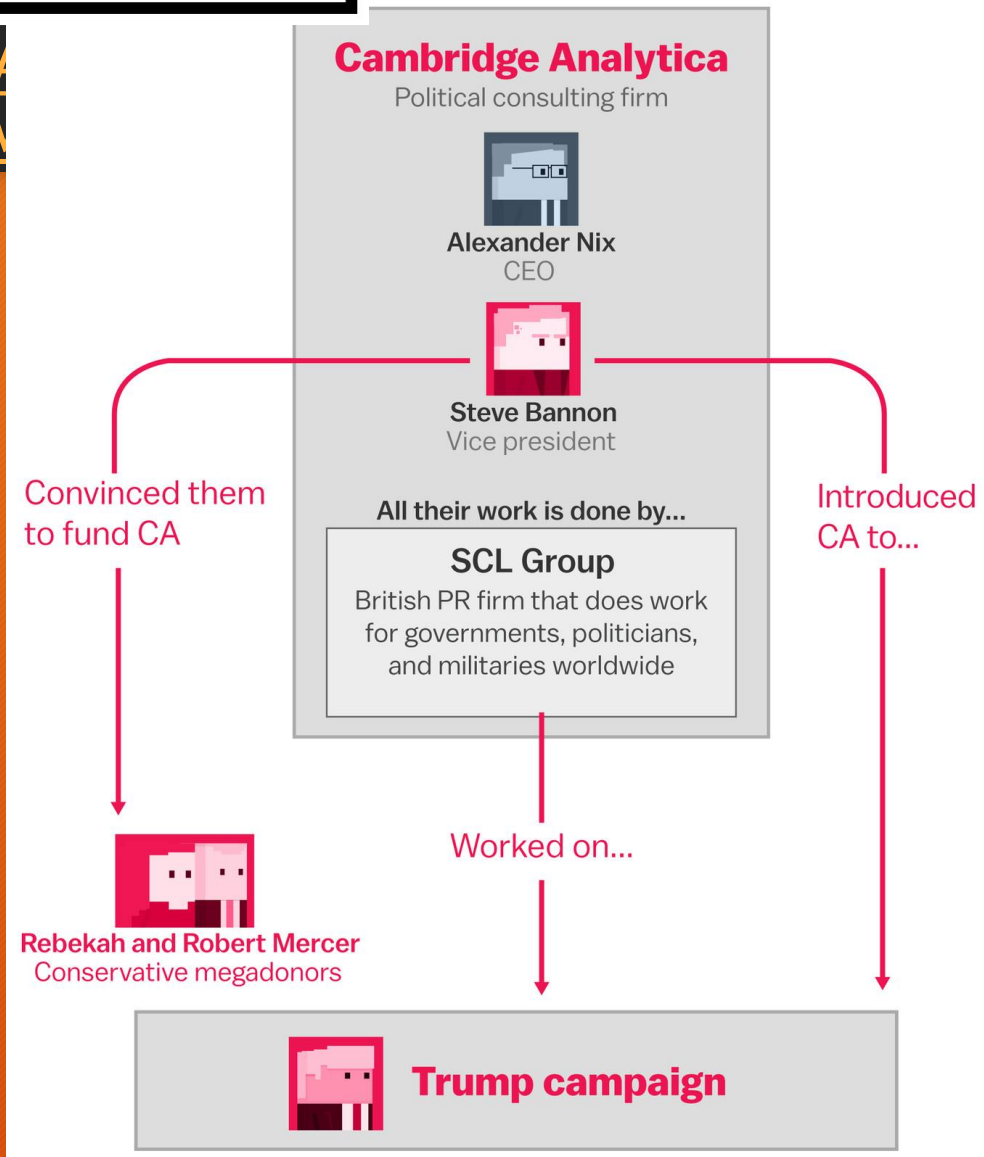
Enter your email address SUBSCRIBE

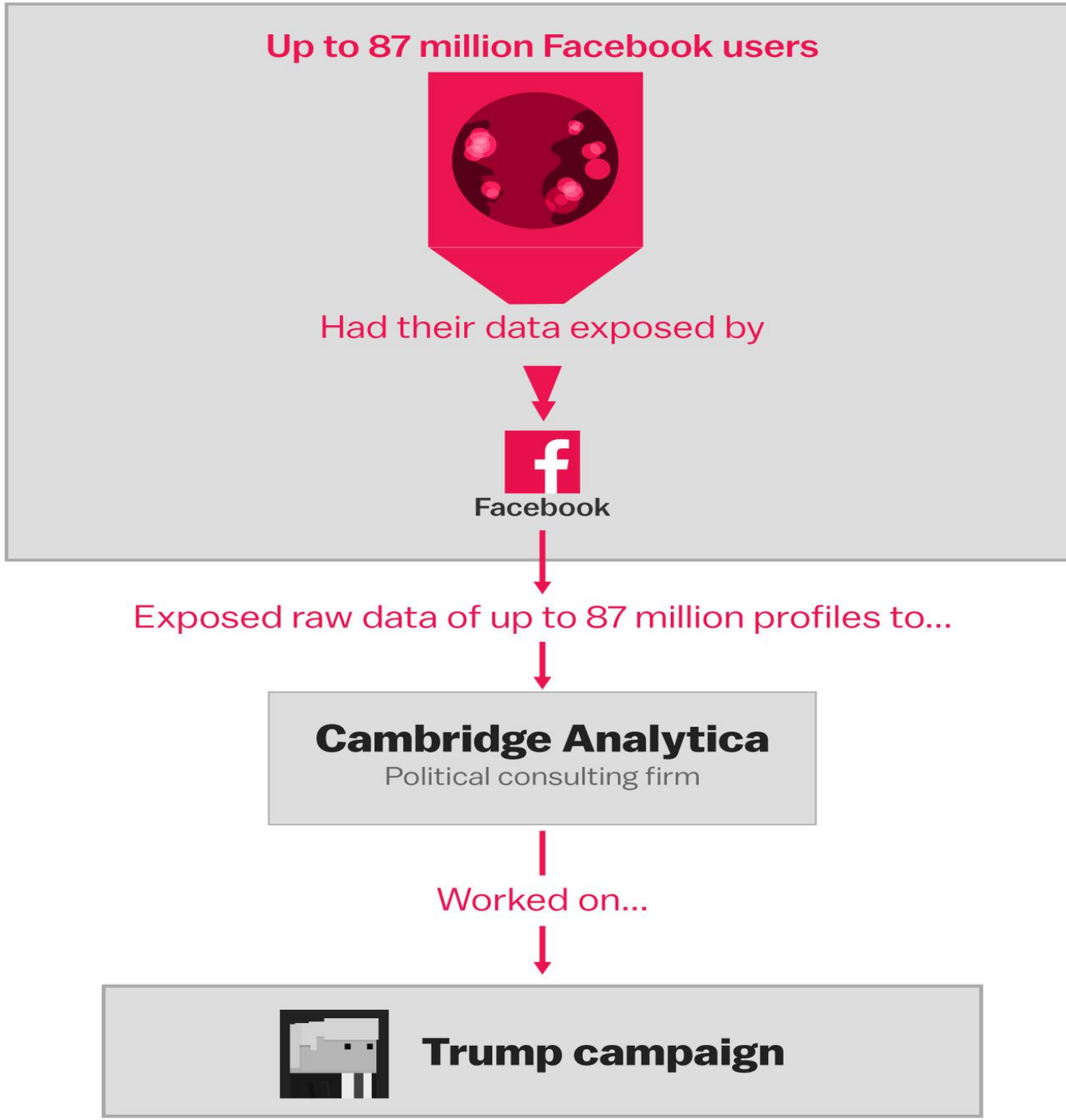
Stay Current

Newsroom
America Counts
Blogs
Stats for Stories

Stay Connected

Facebook & Cambridge Analytica Scandal





Vox
The Facebook and Cambridge Analytica scandal, explained with

How many data point does Facebook have about it’s users?

- **Facebook’s 52,000 data points on each person reveal something shocking about its futu**