The best privacy defense is a good privacy offense: obfuscating a search engine users profile

Joshua Fenech & Omar Salbrout

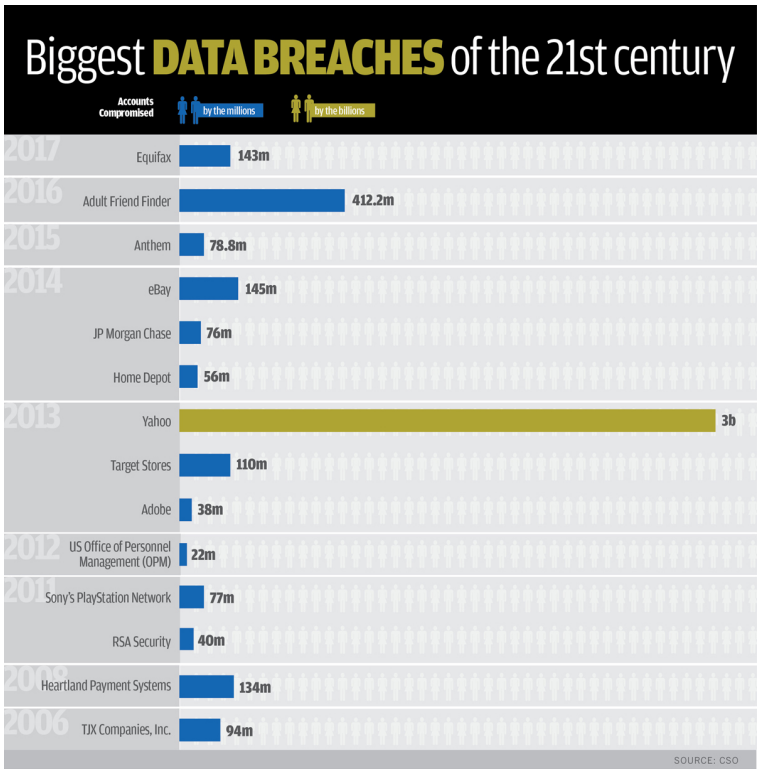
University of Jean Monnet

jfenech22@hotmail.com

December 2, 2017

Overview

Companies can't be trusted



- We trust that companies will protect our data
- Data breaches are commonplace today
- Unencrypted data is often leaked
- There is currently no or little legal requirement to protect data, and therefore represents an additional cost that some companies try to avoid
- Can we encrypt our own data before it is submitted to such companies?

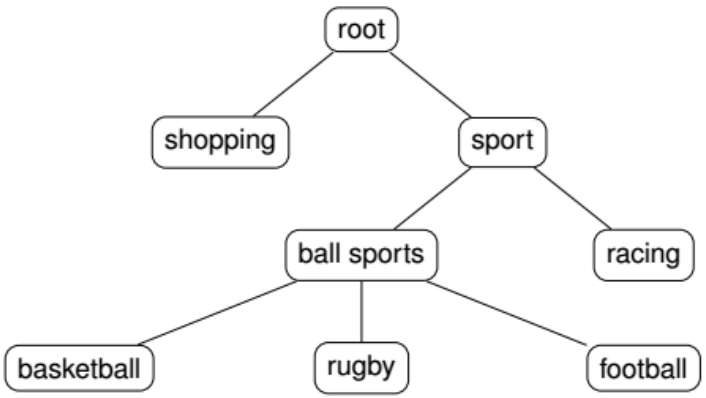
Other methods of obfuscation

- Private browsing - no cookies stored, but... IP still revealed
- Proxy servers to hide IP, but... web browser fingerprints still revealed
- Ultimately, TOR for maximum anonymity
- Problem - lose benefits that personalisation of websearches provides
- Can an alternative means of securing privacy without more intensive [change intensive here] methods be found?

Structure of Presentation

- How do search engines know what we want?
- Present a new method of obfuscation related to adversarial data mining
- Approach is explored in common setting of Internet search engines
- A learning method is presented for environments where a user can get feedback from her or his counterpart

Personalised Advertising



- Which ad is displayed depends on:
  - The submitted query
  - The user profile
- Ads are assigned to categories
- users are assigned to categories

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

References

John Smith (2012)

Title of the publication

Journal Name 12(3), 45 – 678.

The End