The Billion Dollar Product – Online Privacy

Rui Miguel Feio

Security Lead

RSM Partners

Agenda

- Introduction
- Free online services
- Nothing in life is for free
- Paid online web services
- How do they do it?
- Risks
- Security (or lack of it)
- The mainframe
- Conclusion
- Questions

Introduction

- Rui Miguel Feio
  - Security lead at RSM Partners (UK)
  - I am a mainframe technician specialising in mainframe security
  - Experience in other platforms as well
  - I have been working with mainframes for the past 16 years
  - Happy to take questions as we go

Free Online Services

Free online services

- Email services
  - Gmail, Yahoo mail, Hotmail, …
- Web search engines:
  - Google, Yahoo, Bing, …
- Social services:
  - Facebook, Twitter, Google+, LinkedIn, …
- So many others!...

It’s free in return for…

- Placing cookies on your devices to track you and your online activities.
- Collect ‘some’ of your own personal data
- Include ads in the web sites you use

Is this fair?

- YES!! The services are for free!!!
- Who cares?
- I don’t have anything to hide!

Nothing in life is for free

"[…] a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"

– Google's legal team

Privacy Policy & Terms and Conditions

- How many of you ever read them?
- Typically these are extensive and difficult to decipher
- They are legally binding business propositions between you and the online service provider
- Ok, but who cares? It's a free service!!

Let me ask you something…

- How much do you value your privacy?
- How about your friends and family privacy?
- What do you think it could happen if your data was misused?
- Have you ever searched or visited an online website that you would rather keep it as a ‘secret’?

Interesting facts

- On a daily basis Google processes around 24 Petabytes of data. This data is then stored and sold for advertisement.
- Cookies are fingerprints that allow you to be traced and catalogued.
- What you see online is customised for you based on your ‘online profile’.
- Spying on internet users is one of the fastest growing businesses today.

Value of a Company

- Why do you think Facebook or Google are worth billions of dollars?

- A study published by the Wall Street Journal on Facebook:

  - Each long-term user is worth $80.95
  - Each friendship is worth $0.62
  - Your profile page is worth $1,800
  - A business page and associated ad revenues are worth $3.1 million

Let me see if I got this right…

- You use these ‘free’ online web services
- You create your own social network
- You invite others to join the ‘free’ online service
- You add content:
  - Ideas and thoughts
  - Status updates
  - Photos, videos, …
  - Links to other users and pages
  - Interact with other people
  - Search
  - …

So…

- How much do you get paid for all this?
- All of this effort is worth a lot of money for the ‘free’ online service and you get nothing?
- Hmmm… you are indeed a great value for the ‘free’ online service!

Interesting facts

- People who use ‘free’ online services have become the largest unpaid workforce in history!

- The data that you have freely provided can be used by the ‘free’ online service companies to be sold to third parties. You just don’t get any money… and you have no say either!

Paid online web services

Paid online services – are they any different?

- Not really. Many of the paid online services use the data you provide as a mean to capitalise and make more money:
  - Customised services or products
  - Ads
  - Data sold to third parties

How do they do it?

How does it work?

- The online service providers works You out:
  - Reads, scans, and searches your data, messages, emails, and web searches
  - Analyses your data and your online trends
  - Tracks you (cookies, smart phones, …)
  - Creates a ‘online’ profile on You

How does it work?

- The online service providers monetises on You:
  - Tries to sell you products and services based on you ‘online’ profile
  - Displays data on your screen according to your ‘profile’
  - Sells you and your data to third parties

Who would want my data?

- Everyone! Every single company wants it!
- Why?
  - Because now they have a way of profiling you.
  - They know who you are, what you like, what you don't like, what you do, whom do you do it with, who are your friends, your habits…
  - An insurance company knows your habits, and can now decide if you are 'worthy to be insured'
  - A financial bank can decide if it will lend you money or not
  - They now know you!

Risks

Oh, oh, we're in trouble!...

- Who are the third parties that are getting your data?
  - Other companies
  - Data Brokers
- Lack of legislation
- How secure are the IT infrastructure of the companies that now have your data and your 'online' profile?

Danger! Danger!

- Websites, smart phones, tablets, smart watches, GPS devices, …
- How is your data being used?
- For what purposes is your data being used?
- How secure are these websites and devices?

Interesting facts

- 82% of Android apps track and collect your online activities
- Data brokers get information from your ISP, online activity, credit card companies, mobile phone companies, banks, etc.
- Data brokers aim to provide 'behavioural targeting'
- Data broker company Acxiom Corporation:
  - Has more than 23,000 servers
  - Servers collect, collate and analyse more than 50 trillion unique data transactions per year
  - 96% of American households are in its DBs
  - Has more than 700 million user profiles from around the world
  - Each profile has more than 1,500 specific traits
- Former vice president Al Gore dubbed this the 'stalker economy'

Security (or lack of it)

Interesting facts

- Worldwide spending on security software totalled nearly $20 billion in 2012.
- Worldwide spending on security software estimated to reach $94 billion by 2017.
- An average of 62% of the intrusions against businesses were only detected after 2 months.
- The average time from the initial breach until discovery of the intrusion is 210 days.
- Companies face nearly $154 in costs per record stolen.

Costs of data breach for a business

- Detecting the breach
- Containing the attacks
- Investigating the attacks
- Identifying the attackers
- Remediating the IT infrastructure
- Sales decline
- Credit card replacement fees
- Consumer credit-monitoring services
- Insurance premiums
- Drop in stock market share price
- Company’s image

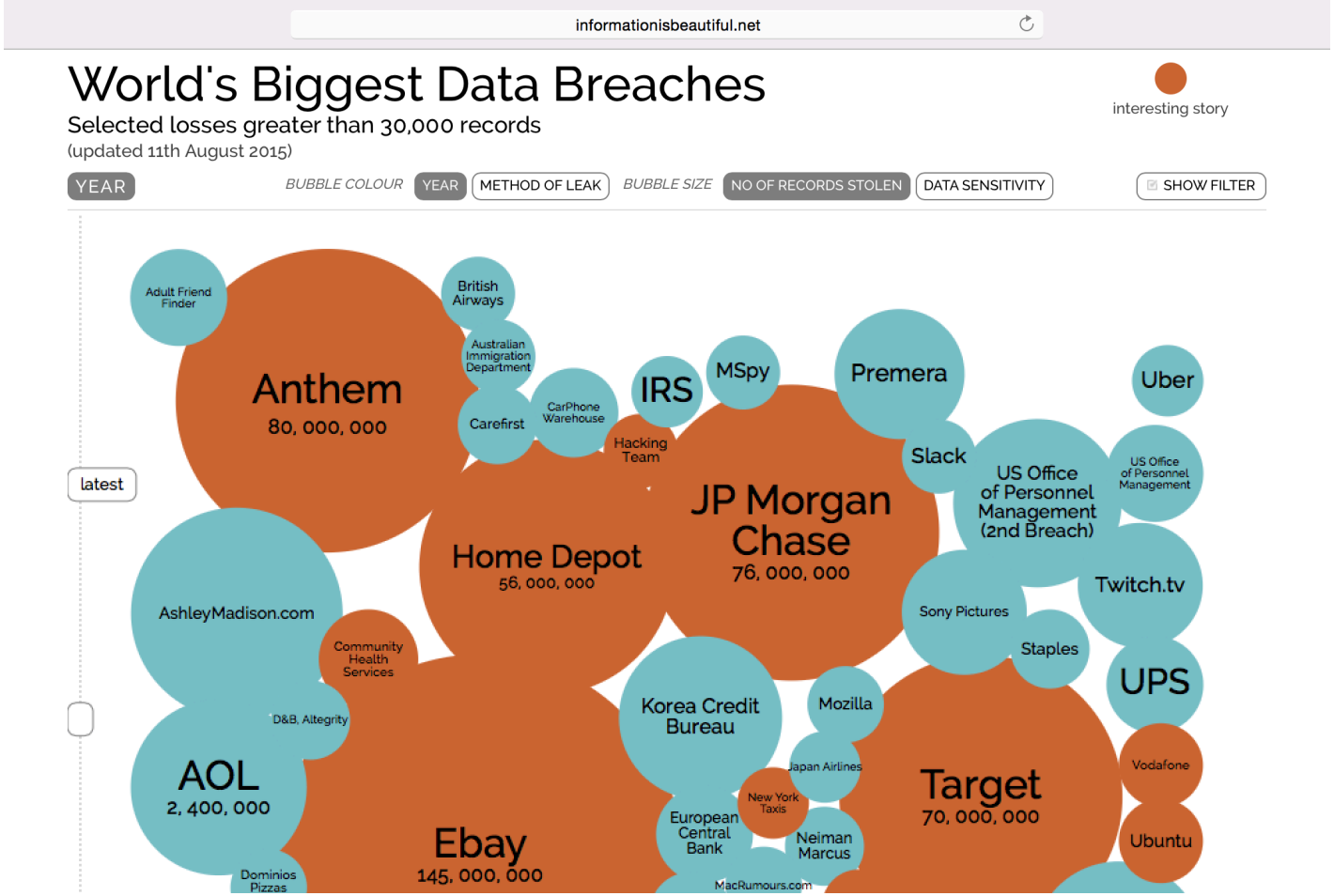
Oh, oh, we've been hacked!

- Carphone Warehouse - 2.4 million personal data (2015)
- Ashley Madison – 37 million personal data (2015)
- Mspy kids & partner tracking service – 400,000 personal data (2015)
- Home Depot – 56 million personal data (2015)
- Anthem health insurance – 80 million personal records (2015)

Oh, oh, we've been hacked!

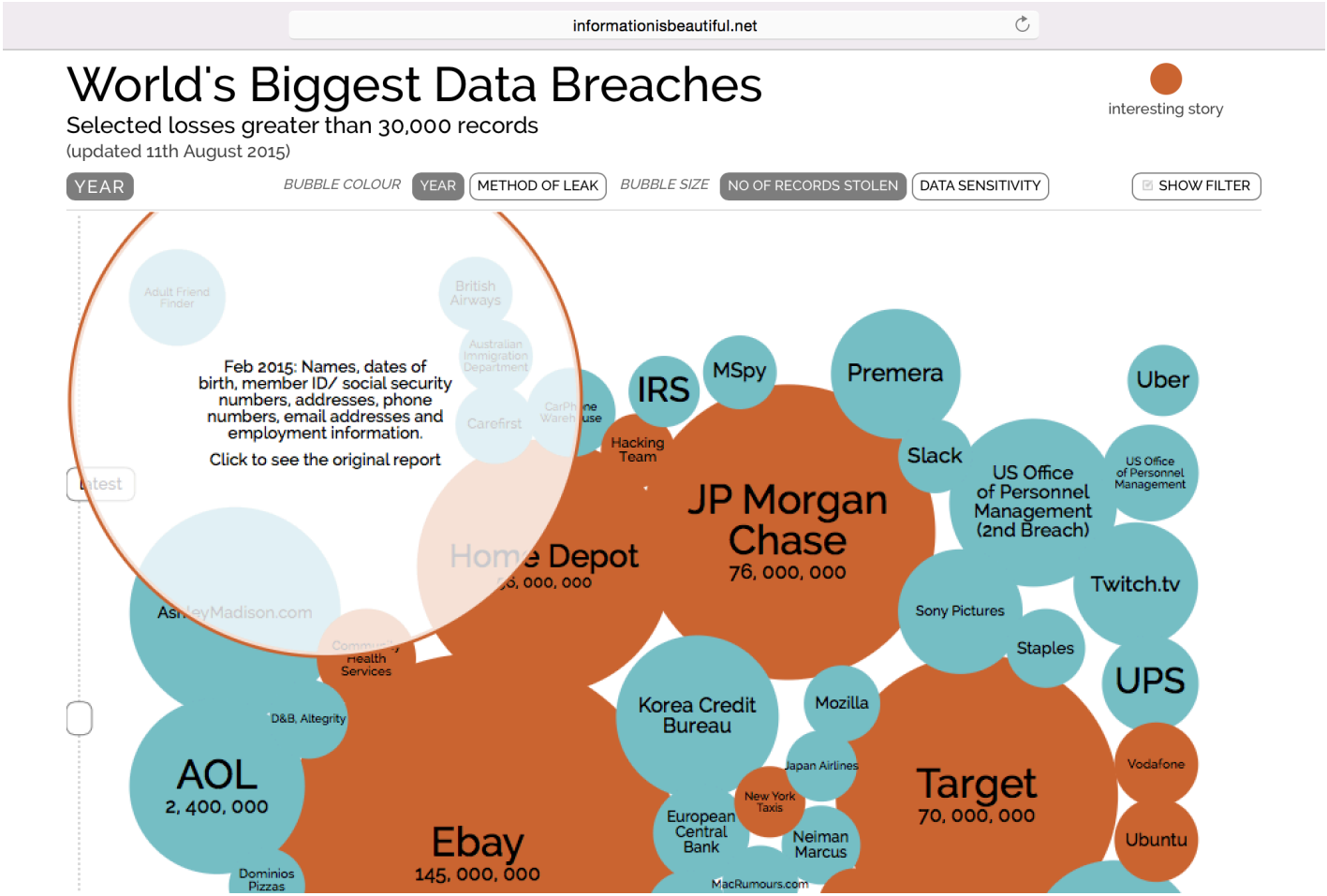
- JP Morgan Chase – 76 million personal data (2014)
- eBay – 145 million personal data (2014)
- Target - 70 Million Stolen Credit Card Numbers (2014)
- Sony Pictures Entertainment – 40GB of data (2014)
- Korea Credit Bureau – 20 million Personal data (2014)
- And so many more!!!

World's biggest data breaches



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's biggest data breaches



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cost of data breach for You

- The hacker can now potentially have:
  - Your online login credentials
  - Detailed information about you
  - Your credit card information

- The hacker can now:
  - Sell your data (yes, even to companies)
  - Test your login credentials in other sites and servers
  - Manipulate your data
  - Steal you identity
  - Black mail you!

So, let me ask you again…

- How much do you value your privacy?
- How about your friends and family privacy?
- What do you think it could happen if your data was misused?
- Are you sure you have nothing to hide?

The Mainframe

Ah, we're safe! No one hacks the mainframe!!

- Are you sure about that?
  - IT firm Logica – more than 10,000 social security numbers (2012)
  - Swedish Nordea bank – personal data, money (2013)
  - Internal hack in one major UK Bank (2013) - £2million in losses

- But the mainframe is the most secure platform in the world!
  - No, the mainframe is the most securable platform in the world
  - Requires work around security
  - Resources
  - People need to be trained to be kept up to date to the new security threats and trends

From my experience with mainframe clients…

- The mainframe is part of an ecosystem of other platforms.
  - If one of them gets compromised how will it affect the mainframe?
- Hackers are getting really interested on the mainframe.
- It's just a matter of time until the mainframe is seriously compromised.
- Oh my, a lot of work needs to be done!

From my experience with mainframe clients…

- Management still sees the mainframe has un-hackable which leads to lack of investment or interest in security
- While doing mainframe audits and penetration testings on different clients, the same common security problems are being overlooked and not addressed.
- Most mainframe sites do not have not done a proper data classification.

Conclusion

Conclusion

- ‘Free’ online services can be useful. Use them, but don’t abuse them!
- Think: “Do I really need to use this service?”
- Be careful about the data you provide!
- Others can pick your digital footprint and interpret it without your knowledge and in ways that can cause you harm.
- Governments need to implement appropriate legislation around data and privacy!
- Private data is worth billions!

Questions

Contact

Rui Miguel Feio
RSM Partners
ruif@rsmpartners.com
mobile: +44 (0) 7570 911459
www.rsmpartners.com