James Smith - 863266

How Safe is our Online Data?

CS-130

Introduction

In this report I will be looking at all the ways our data is handled online. Covering who is able to access personal details to how it is protected Then to how it can be collected without us even knowing and finally what can be done to protect sensitive data ourselves.

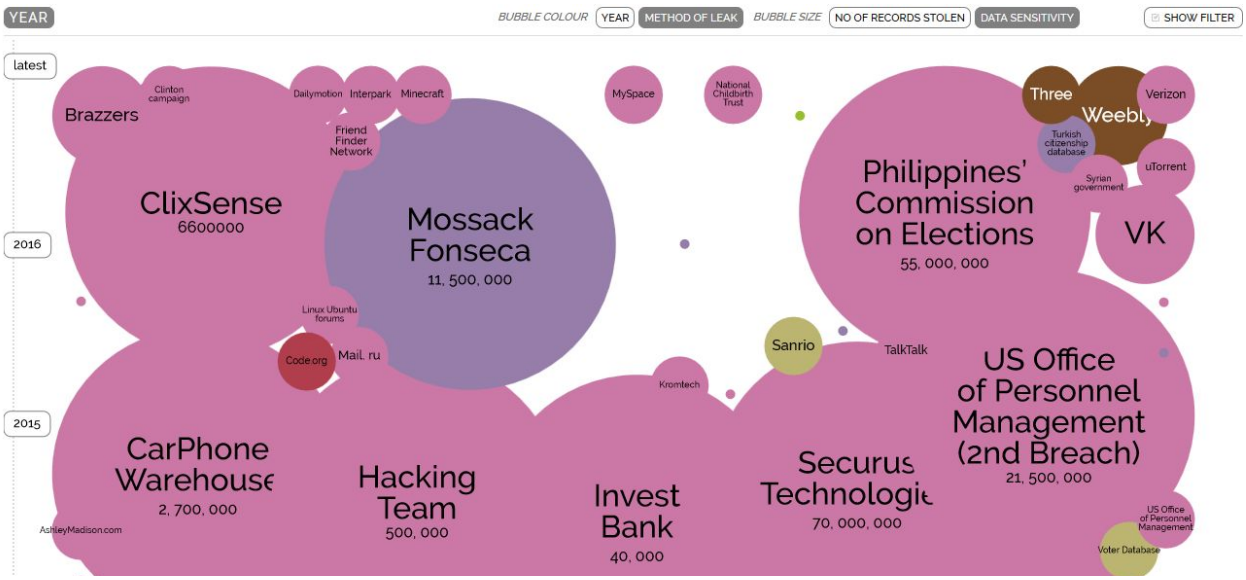
Who has access to your data?

In this first section we will be looking at who has access to your data *and how much of it they can see.* We start by looking at a well known location personal data ends up. Companies we willingly hand information over to. This includes; social media, dating sites and often several online retailers.

With social media websites such as facebook and twitter the common user is quite happy to give away personal details about themselves. They want their friends to see what they are up to. They want to show themselves off in the best possible light. The same goes for dating websites. Some of the data given up can be quite personal and while most think what we share is harmless (after all it's not your bank details or home address you are posting online) information such as hobbies and interests can still be of value. Should we trust these companies to protect our data? It is well documented that Facebook sells user data onto third party advertisers [1][2][3] for profit. Facebook says it's doing this so that users can enjoy a more relevant "*ad experience*," but in reality it's because our data is like gold. Once advertisers know interests and online habits they can target prospect customers directly for a more effective ad campaign. This leads to companies owning data which we would not normally consent to. This is technically legal. The terms and conditions state clearly [4] they will be doing this but the average user will not read the

large document and therefore be unaware. This is not what we want to happen with our data. Unfortunately there is nothing that can be done to prevent this apart from not enter personal data online although as we all know this can prove a challenge in the internet age. Hopefully the new UK data laws that will be put in place due to the EU referendum[5] will change this for the better but for now we can only hope.

This covers the lawful acquisition of data but there are also unlawful practices taking place. Just this year there have been twenty large cases of data breaches online [6]. This is only counting very high level companies and does not even include all small scale unreported businesses. One of the largest examples was the February breach of the US department of Justice. "*The hackers released data on [30,000 employees over two days] . Information stolen included names, titles, phone numbers, and e-mail addresses. Tweeting from the account @DotGovs, the hackers said it took one week for [the DOJ] to realize their systems were compromised*."



Data visualisation of large data breaches over the past two years [7]

We trust online companies with our data and to keep our passwords safe but there is no totally secure service. Banks, Social media sites, online games and governments have all been breached.

Passwords

Passwords are used for everything online. There is no way of avoiding them if you intend to create an account to use a service. They allow us to keep our sensitive data safe online. All text messages, money, photographs and entire identities. Everything you store online is protected by a few lines of code and on average a 8 character string which, and as studies suggest[11], 60% can be cracked within minutes. There are two methods to obtain someone's password, If the criminal has a specific target in mind they will use a more direct approach, such as phishing, man in the middle or sniffing attack.

Phishing is quite widespread as it requires the least technical. It involves the sending a spoof email or webpage to the target. Pretending to be the bank or another service provider they ask you to login to what appears to be official page when in fact it’s a counterfeit which sends the entered details straight back to the hacker. A recent example of this is the fraudulent 'speeding fine' email phishing scam [8] in the manchester area. Luckily the Police promptly managed to release a warning to the public.

The other weakness is how the passwords are stored by online businesses. In some cases the storage of passwords has not included any encryption. This can have major repercussions as seen in the Adobe scandal of 2013 [9] where the leak contained millions of users unsecured passwords. This is why passwords and other sensitive data should be encrypted if not hashed using a salt.

Passive Data Collection

In this section we will take a look back at who is collecting this data and take a more indepth look at why.

Most online business retailers collect your data, even if you don’t input anything. The way they do this is tracking cookies. Using these it allows businesses to advertise more effectively to you. When looking to buy a new appliance, such as a fridge or dishwasher online, the tracking cookie would allow them to register this and then advertise to you in banner ads on other websites you visit. This can be seen in the case of with American company Target advertising maternal products to a pregnant teen girl before her father

knew she was pregnant. [10] Using algorithms on their store purchase data they could make a link between certain products such as unscented lotion and large bags of cotton wool to separate stages of pregnancy. This means that they could even tell which trimester the customer was in.

Again this is just the legal side of online tracking and data collection. There is also a much more sinister method used by criminals to follow your web habits and gain your details without you knowing. Looking back at unsolicited emails there is another practice used with spam emails. Rather than phishing for your login details they can embed keyloggers and other malicious software into web pages which discreetly install onto your hard drive. This can be in the form of misleading software ie Rogueware or in the background. Once installed this malware can wreak havoc on a system or lie dormant logging keystrokes.

There is also a grey area when it comes to certain forms of online surveillance. This comes when you allow particular forms of data to be collected for one purpose but is then used in another. This can be best show with an example. If a customer of the Bank of America downloads their companion app is asks for permission to use the camera and microphone. This is because they feature a security system whereby if an incorrect attempt is made on your account a picture is taken of the unauthorised user. While this service may seem useful it also means the bank have the ability to listen in 24/7. They may not do this themselves of course but with the case of a rogue employee or even hacker they have immediate access. It can get even more disturbing than that. With GCHQ and the NSA being sections of governments in the UK and US respectively, legal loopholes allow them to have access to any mobile device or computer and track your every movement[12]. While this is portrayed as an act of public safety and civil protection it also requires us to relinquish our privacy. There is much debate around this as privacy is an innate right. Can this act by our governments be deemed extreme and unreasonable?

How can we protect ourselves?

While the debate for internet privacy and Government access is ongoing there are several ways to protect yourself in the current digital age.

All common operating systems offer a way of encrypting your hard drives and storage devices, if not there are many third party options available online. Encrypting hard drives gives you an extra level of digital protection.

Looking back to password usage, with the studies have suggesting that most could be cracked within minutes we need to rethink how we decide what to use. The more appropriate term would be ‘Passphrase’. A long string of characters is hard to remember but if made into a phrase or story the human mind is much more likely to recall it easily.

Disabling tracking cookies is another way to hide your online presence. There are several options offered by common browsers [13]. This means both useful online web store cookies and unwanted harmful cookies will not be stored. For deeper online protection you can use various other methods and applications. Some popular choices are to use a VPN, Tor Browser and enabling end to end encoding in common messaging apps.

Word Count: 1496

Bibliography

[1] http://time.com/4695/7-controversial-ways-facebook-has-used-your-data/ [News Article]

[2] http://www.makeuseof.com/tag/facebook-selling-data-mean-privacy/ [News Article]

[3] https://actions.sumofus.org/a/Facebook-selling-user-data [News Article]

[4] https://www.facebook.com/full_data_use_policy [Policy Documentation]

[5] http://www.bbc.co.uk/news/technology-36037324 [News Article]

[6] https://www.identityforce.com/blog/2016-data-breaches [News Article]

[7] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [Data source]

[8]http://www.manchestereveningnews.co.uk/news/greater-manchester-news/police-issue-warning-over-new-12283129 [News Article]

[9] http://www.alphr.com/news/security/385270/adobe-hack-152m-records-found-leaked-online [News Article]

[10]http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did [News Article]

[11]https://www.youtube.com/watch?v=7U-RbOKanYs [Data Source]

[12] https://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world [News Article]

[13]https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=en [Technical documentation]