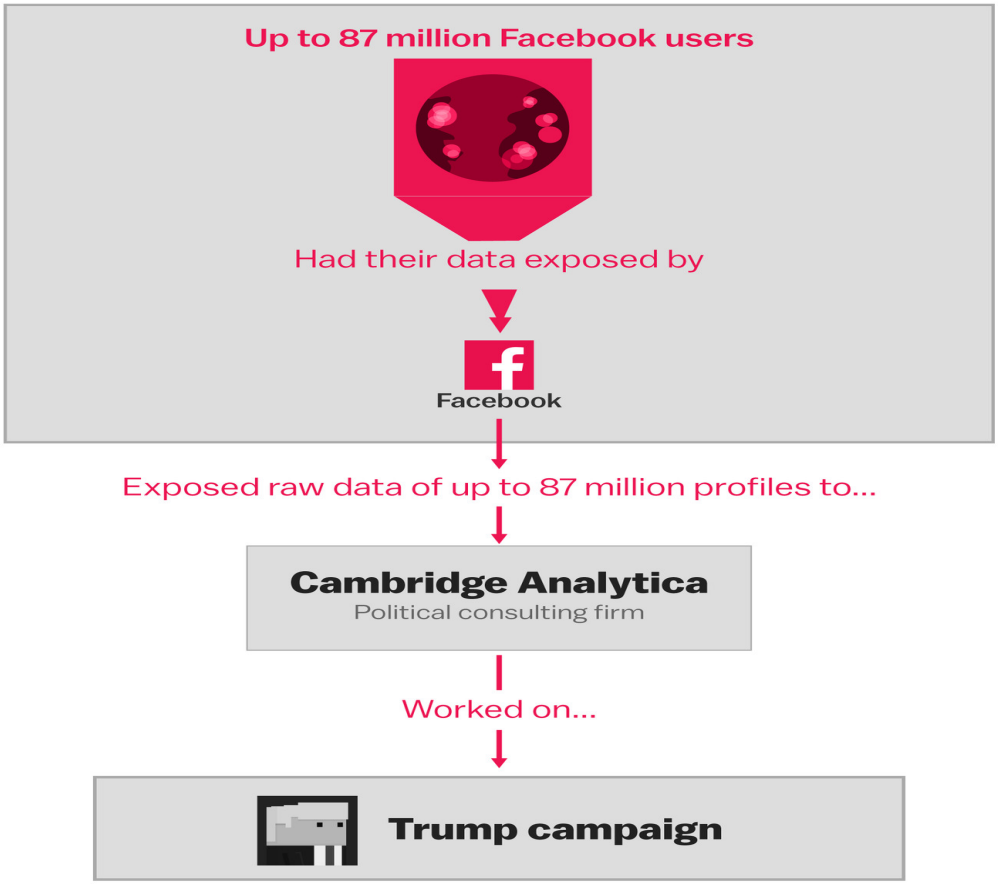
DATA PROTECTION AND SOCIAL MEDIA

FACT SHEET

As social media becomes an increasingly important part of life, it has become common knowledge that businesses are finding ways to manipulate your data and digital footprint to influence your decisions and their profit margins.

However, what people may not be aware of is how they can be micro targeted to influence the democratic process. Companies such as Cambridge Analytica harvested the data from 87 Million Facebook users to target persuadable users to vote for their client during campaigns, resulting in following shock results:

- Trump 2016 Election Campaign



The accuracy of predictions that big data companies can make by using your personal data is alarming. In 2013 researchers from the University of Cambridge published a paper explaining how they could predict personalities and other sensitive traits from freely available Facebook likes.

In 2014, Professor John Rust of the University of Cambridge wrote a letter to the University's head of legal stating that Aleksandr Kogan, a key figure in the Cambridge Analytica scandal, was "using an app he created to collect data on millions of Facebook users without their knowledge." The truly alarming point was not only did the app collect data on people who opted into it, it also collected data on those users' Facebook friends.

For example, if 100,000 people opted into the app, and if they had an average of 150 friends each, you would have access to 15 million people's data, which you could then use for the purposes of political persuasion.

Well documented and publicised scandals, such as Cambridge Analytica, and lesser know and currently developing cases like Lifecycle Marketing (Mother & Baby) Limited, have thrust the recently implemented EU **General Data Protection Regulations** (GDPR) in to the spotlight.

GDPR - LEGAL PROTECTION

GDPR, a vital part of EU Legislation, dramatically limits how organisations can use your data. It simply ensures that users can control which information is shared with companies. It also imposes harsher penalties against organisations who are found to be guilty of a data breach, when compared with the previous Data Protection Act 1998.

The cleverly designed piece of legislation has global impact;

- The Brussels effect, governments outside the EU adopt the principles of EU legislation due to the gravitas it can hold.
- It binds organisation operating outside of the EU if they are processing data inside member states

Key Principles of legislation:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

GDPR Protection for Social Media Users

The effect of the legislation is increased privacy and better security for social media users. The core impacts on users are as follows;

You have the "right to be forgotten", i.e Erasure of all data when asked. Art 17 (GDPR)

Plain language must be used in all privacy policies and in explanations of how data is being used. Art 12 (GDPR)

Clear consent is required to collect and use users' data with easy ways to opt out of some or all data collection. Art 4 (GDPR)

You must be informed of a security breach within 72 hours of its detection. Art 33 (GDPR)

You have to be given the right to opt out of target advertising using their personal data. Art 6 (GDPR)

Special safeguards should be in place for information related to race, sexual orientation, health, religious and political beliefs. Art 9 (GDPR)

In addition, there are increased consequences for data breaches. Under the Data protection Act 1998, the maximum fine against a company was **£500,000**, which is what Facebook was ordered to pay as part of the Cambridge Analytica inquiry. Under GDPR, companies can face up to €20 million in fines, or up to 4% of global annual turnover. If Facebook were to receive the same fine under the new legislation, they could have been fined 4% of £1.4 billion: **£56,000,000**

Trouble on the Horizon?

GDPR has increased social media users privacy and security online. However, it it potentially threatened by Brexit, with questions raised of the applicability of GDPR to UK companies putting distance between us and our newfound security.

The Threat

As the UK moves out of the EU at the end of 2020, Google has announced plans to move UK data and user accounts from Ireland to the US.

The reasons for the shift are as follows;

- Uncertainty if the UK will adopt similar measure to the GDPR post 2020
- If data is kept in the EU, British authorities would struggle to recover it for use in criminal investigations
- Tech companies don't want to be caught to be caught between two governments

Other tech companies, such as Facebook, which operate in a similar fashion to Google have not commented on future plans, however this could be the start of a trend among tech giants.

Moving user data from the EU to the US will drastic impacts upon security. The US has some of the most lax data protection laws, and virtually none are applicable for non US citizens,

The **Clarifying Lawful Overseas Use of Data Act** or **CLOUD Act 2018,** is a US Federal law enacted in 2018, and is expected to make the acquisition of data by British law enforcement agencies easier as the two nations negotiate a more comprehensive trade agreement.

The Data Protection Act 2018

The DPA offers some hope, as it reflects the UK government's commitment to the creation and enforcement of strong data protection laws.

It forms the basis of absorbing the GDPR in to domestic law, and the beginning of creating an adequacy agreement with the EU once it has left the bloc. However, such an adequacy agreement can only be finalised once the UK is no longer a member state of the EU.