GET1004/GEK1531
Cyber Security Report
AY17/18 Semester 2
GROUP 47

Personal Data Protection: Who should take charge?

Group Members

Kelvin Tan
Loh Jia Qing
Neo Yin Lin
Leow Shirlene
Teo Meng Shin, Ryan

Introduction

According to the Personal Data Protection Commission (PDPC), personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access (2018). As we move towards a new digital era, personal data is highly sought after by companies in order to provide customised experiences. However, one must be wary of whom he/she is sharing their personal data with as there are individuals or companies who might disclose or misuse such data. In light of this, there has been a constant debate about who should be responsible for the protection of personal data — the individual, the organisations or the governments. Hence, it is important to identify the major stakeholder in protecting personal data to put an end to complacent behaviour in order to move from blame to accountability.

This report aims to explain the following key issues related to personal data:

1. The importance of protecting personal data

2. Exploring how personal data is valuable to companies

3. Identifying who should be the major stakeholder in protecting personal data

Importance of Protecting Personal Data

We shall first begin by explaining the importance of protecting our personal data by exploring how it can be potentially misused.

Living in the information age with most of our interaction on the internet, it is easy to unknowingly disclose our personal information. The rise of the “Internet of things” and increasing ownership of mobile phones has allowed a massive amount of personal information being made available online. However, many of us fail to realise that the information we provide online are essential for cyber crime to occur, some of which are highlighted below.

Fraudulent use of Financial Data

Fraudulent use of credit cards is increasingly common with credit card information made readily accessible. According to data compiled by ACI Worldwide and Aite Group, it has been noted that fraud rates are increasing in many countries (Knieff, 2017). With a rapidly-expanding global e-commerce market, online shopping has become increasingly convenient.

However, this effortless experience can sometimes leave consumers’ financial details vulnerable to criminals, especially if risky consumer behaviours are present. Risky consumer behaviours include online banking and shopping without security software or responding to emails asking for financial information. Such behaviours allow hackers a chance to intercept the transactions and steal financial data. With the stolen data, hackers can either use the data for illegal transactions or sell it at high prices through online markets such as the AlphaBay Market (Aw, 2017). Ultimately, not only would the affected individual suffer a financial loss but their credit rating might also be affected.

Internet of Things Spying

The fast-expanding and highly anticipated technology - Internet of Things (IoT) provides us with greater interconnectivity and convenience. Development of IoT, includes devices like Google Home or devices like Piper NV, a video monitoring and home automation device that allows users to stay connected to their homes through the piper application (Bell & Merriman, 2015). Such devices bring about great benefits to the consumers such as child monitoring when an individual is at work. With such convenient features, the adoption rate of IoT devices is expected to grow rapidly, with Gartner forecasting that by 2020, there will be at least 20.8 billion such devices (2017). With greater interconnectivity between the devices and the internet, it is easier for manufacturers, intelligence agencies and even internet service providers (ISPs) to be spying on device owners without their knowledge.

For instance, ISPs could spy on your in-home activities by analyzing the internet traffic of your devices. Recently, US intelligence agencies have also declared the plausibility of them using IoT devices for surveillance (Ackerman & Thielman, 2016). This puts us at risk of having our privacy invaded as IoT devices could allow the passive collection of data. Moreover, there is ambiguity in who the collected data is shared with; meaning, collected data could even be shared with third parties without the users' knowledge. Furthermore, due to the massive amounts of IoT devices present, it would be hard to keep everything secured. Hence, there will always be unsecured IoT devices which hackers would attack and spy or retrieve personal data on individuals.

IoT security is often overlooked by many individuals as the risks are not as apparent as the theft of financial data. For example, hackers could use the IoT devices to analyse an individual's habits in order to determine the optimum period to rob their home.

Identity Theft / Fraud

As we rely more on the internet, new risks emerge as we perform a wider range of transactions online and readily share more personal data online. Computer hacking and social engineering scams, more commonly known as phishing, could be carried out by criminals to illegally obtain personal data from us. Computer hackers could hack into computer networks to obtain confidential data while phishing is a method that tricks people into providing their personal data to a criminal who masquerades as a legitimate organisation. Hence, as individuals, we should always take precautions whenever we share data online. Otherwise, this could lead to serious crimes like identity fraud and theft. Javelin stated that stolen social security numbers were more than credit card information in 2017 (O'Neill, 2018).

This is a problem for the individual as with the stolen identification data, criminals could make false applications for loans and credit cards, make fraudulent withdrawals from bank accounts or commit crimes under the stolen identity. Criminals can even make use of the benefits from another person's identity such as obtaining goods or privileges which the criminal may have been denied access if they were to use their own name. An example of such would be a tax refund fraud, whereby the criminal would claim the refund illegally in place of the individual.

Identity theft and fraud can possibly take a long time before any discovery comes to light. To further heighten the issue, it takes time for recovery of identification for the victims. Clearing of the victims' would be challenging and the victims' finances would typically be the most adversely affected.

How Personal Data is Valuable to Companies

Data is knowledge, knowledge is money. The more data a business collects, the more money they will make. We are living in the era of Big Data where modern business environments are flooded with data. As technologies such as the IoT and artificial intelligence (AI) continue to develop at a rapid rate, companies have begun to collect and analyse increasing amounts of data.

From seemingly harmless information such as name and addresses to sensitive ones such as credit card numbers, companies are attempting to collect all of your data. Every time we log onto the web, watch a video on YouTube, do a google search or make a purchase online – information is being collected.

Benefits of sharing of personal data

While many may have reservations about sharing their personal data with service providers, there are actually some benefits for those who do. Companies could make use of the data to generate valuable information for the company and individual. For example, Google has an option for users to share their location history. On one hand, some would refuse to share such sensitive information as it would be tantamount to spying. On the other, those who do share their location history benefit from suggestions or traffic alerts with regards to their daily commute (Google, 2018). Similarly, Facebook also has an option for users to share their contacts. There are users who might be reluctant to share their entire contact database in order to protect the information of their contacts. However, those who do share their contacts get to enjoy the benefit of seamlessly inviting them to their social network profile (Facebook, 2018).

Collection of consumers' data is especially useful for targeted advertising. By retrieving information on an individual's click history and browsing history, companies can interpret the data and display advertisements targeted to his interests. A 2009 study has

shown that the click-through rate of an advertisement could increase by 670% through behavioural targeting. (Yan et. al, 2009) This means that companies could enjoy more cost-effective advertising by using personal data wisely. Consumers can also enjoy the benefits of more personalised services and the convenience of having relevant information presented to them. Advertising on the internet can also offer free content for consumers. The costs of designing and managing a website or an application is paid for by advertisers, thus consumers can enjoy free services and content online. Often, websites and application developers would offer an option for consumers to pay for an ad-free version if they were to find advertisements distracting or annoying.

While we acknowledge that collecting data is helpful to both consumers and businesses, problems arise when privacy is invaded and when sensitive data is compromised, causing consumers' to be vulnerable. All these issues highlights the importance of protecting consumers' personal data. Hence, sharing of personal data online may have its dangers, but effective usage of it does bring convenience for people willing to take the risks.

Who should be the Major Stakeholder in Protecting Personal Data?

Why should individuals protect their own data?

Many are aware of the risks to our personal data. However, most favour convenience as opposed to the perceived hindrance by being more cautious. Thus, most simply ignore these risks or leave the data protection to external organisations and expect them to be accountable for anything that goes wrong. After all, most governments are holding organisations responsible for data protection through legislation, such as data breach disclosure laws or data protection acts.

However, we cannot blindly place our trust on individuals or organisations to keep our data safe. For example, it was recently revealed that a Cambridge University researcher, Aleksandr Kogan, used a Facebook app to harvest profile information of Facebook users and shared it with Cambridge Analytica without their consent (D'Onfro, 2018). In this example, Mr Kogan had abused the trust placed in him by numerous Facebook users. This highlights the fact that we should not always assume that external parties have our best interests at heart.

In addition, most banks only waive liability fees of victims of financial fraud only if the necessary precautions have been undertaken by the victim. For instance, DBS only guarantees the protection of customers' funds if their recommended security practices are adhered to, some of which include keeping antivirus software up-to-date (2018).

This reaffirms that it is important for individuals to take the first step to protect themselves first, instead of solely entrusting the security of our data to organisations.

How can individuals protect their own data?

One solution to protecting their own data is to first protect their own identity. This is done by safeguarding the personal information that we share online. A simple way would be to activate the two-factor authentication (2FA) option. 2FA simply implies that there is a second layer of authentication on top of having a password. Common 2FA options could come in the form of an One-Time Password (OTP) token, SMS and even smart cards. Let us compare the differences between some of the more common 2FA options.

OTP tokens generate one-time passwords to allow for log in, it provides a good balance between privacy and convenience. As the secret key is in the device itself, it cannot get intercepted easily. However, most tokens require internal clock syncing and if a hacker manages to clone the secret key, they would still be able to bypass the OTP authentication.

SMS would be the most convenient as the individual would not need to carry a physical token around. A SMS will be sent to a registered mobile number containing a security code required for verification when making online transactions or using social media sites. Alternatively, if there is no mobile network, one could even download an authenticator application such as Google authenticator. This will generate time-based verification codes without the need of a mobile network. This is similar to that of an OTP token, the difference being that the “token” is now your mobile phone. However, it is possible for a hacker to intercept a SMS or tokens generated by an authenticator application if an individual’s mobile phone has been compromised.

Smart cards use the universal 2nd Factor authentication which is the most secure as they are phishing-proof and cannot be intercepted. However, they are very costly and typically not feasible for use on a large scale, except for extremely sensitive data.

2FA provides an additional layer of security to having only a password by ensuring that only you can have access to your own account. This helps to reduce the risk of someone else being able to steal your information or identity.

In addition, having secured devices and networks also brings about additional protection to one's data. To have a secured network, ensure that the network is encrypted with a password and that the network is using the existing WiFi protected access (WPA2) protocol. This ensures that any information transmitted is kept confidential and that it would be challenging for others to have access to your network to steal information. Although WPA2 may not be perfect in protecting the network from hackers, it implements the latest security standards, which make it harder for hackers to gain access (Pinola, 2017).

Why should organisations protect consumers' personal data?

Data privacy and security have become a major area of concern for companies and organisations. Organisations that have failed to take the necessary precautions in protecting consumers' personal data are facing potential dire legal consequences.

In the United States (US), the Federal Trade Commission (FTC) is filing complaints against companies that failed to uphold their promises in protecting consumers' personal data. In 2017, FTC and Uber settled a privacy complaint that alleged Uber had failed to act in accordance with its promises to protect consumer and driver data from improper employee and third party-access. As part of the settlement, Uber will submit to twice-yearly privacy audits for the next 20 years (Sterling, 2017).

Moreover, companies across the globe are collecting consumer data for the application of AI. AI can be divided into many fields, such as natural language processing, robotics and machine vision. Companies across different fields are trying to tap onto the prowess of deep learning models to make use of the abundance of data. For example, fitness monitoring devices such as Fitbits utilise artificial intelligence to aid consumers with chronic health conditions such as diabetes and cardiovascular disease (Roderick, 2016). Some companies even give out Fitbits to their employees to gather data for use in employee medical insurance purposes (Provazza, 2017). This often includes the use of sensitive consumer data, which comes with privacy implications. A survey conducted by KPMG concluded that over 90 percent of consumers felt like they had no control over the way organisations handle and use their personal data (2016).

It is evident that an increasing amount of consumers becoming aware of potential privacy issues. In order to ease consumers' concerns with regards to their personal data, companies should make use of this opportunity to make assurances of data privacy and security to build consumer trust.

How can organisations protect consumers' personal data?

One solution to the issue is through the application of masking on consumer data. This involves hiding sensitive consumer information during data analysis, such that the privacy of consumers is preserved. By minimizing data collection and retention, this will also reduce the risk of the data being compromised. Several studies have been performed on techniques to develop accurate models without accessing individual data records with reasonable accuracy (Agrawal & Srikant, 2000).

Another practice that companies can implement to improve the security of their customers' data is safe data storage techniques. One key aspect in safe data storage is authentication. Authentication restricts access to the data. Multi-factor authentication (MFA) can be used to prevent break-ins (Banyal, Jain, & Jain, 2013).

Another aspect is to prevent data breaches from within the organisation, typically by employees that have the authority to access the data. Employees could have used personal storage devices like USB memory sticks or iPods to obtain sensitive information from the company for malicious intent, commonly known as "pod slurping". Additionally, employees could also obtain information from the company through a bluetooth connection, known as "bluesnarfing" (Rolls, 2008). This can be mitigated and prevented through internal management systems such as keeping logs, regular monitoring and audits. The organisation could also implement a multi-level security policy within their network. This would restrict access only to data required by the employees to perform their duties and nothing more. This reduces the risk of personal data being stolen and facilitates investigations by narrowing down the possible suspects who might have misappropriated consumers' personal data.

Last but not least, companies should obtain a SSL certification from a trusted Certification Authority such as GlobalSign. SSL certification uses public key cryptography which has a public and private key. This prevents a hacker from

intercepting and obtaining consumer's data or information that is meant to be shared only with the company over the internet.

All of the above help in keeping data secure and builds consumers' trust in the organisation knowing that their personal data is secure.

Why should governments protect consumers' personal data?

A possible regulator of personal data protection and privacy could be the respective governments or legislative authority of each country. Respective legislations could be enacted such that any organisation involved with the "collection, use, disclosure and care of personal data" (PDPC, 2018) have to abide by a strict set of guidelines when handling personal data. Organisations which fail to do so would then be subject to enforcement action.

In the European Union (EU), the General Data Protection Regulation (GDPR) goes into effect in 25 May 2018 (EUGDPR, 2018). Ranging from requiring the consent of consumers for data processing to providing data breach notifications, the GDPR requirements aims to create protection on consumer's personal data across EU nations. As a whole, the GDPR provides an official benchmark for companies that are collecting and storing EU citizens' data.

Thus, governments or legislative authorities are in a key position to ensure organisations do their due diligence to protect data through deterrence.

How can governments protect consumers' personal data?

CASE STUDY: SINGAPORE

An example of such a legislation would be the Personal Data Protection Act 2012 (PDPA) in Singapore. The PDPA takes into account 3 key concepts in data protection: consent, purpose and reasonableness. It is also all inclusive as these regulations apply as long as the data was collected, used or disclosed in Singapore, regardless of the origin of the organisation. (PDPC, 2018).

Organisations which fail to meet the standards set by the PDPA or suffered a data breach would then be subjected to enforcement, ranging from the cease of use of personal data in contravention of the act to a financial penalty (PDPC, 2018). For example, organisations which failed to protect personal data were issued fines while other organisations which did not meet the required standards of the PDPA have been issued warnings as part of enforcement action carried out by the PDPC (Cheok, 2016).

It must also be noted that some organisations may try to trick individuals into granting their consent for their data to be used freely and without restriction. This is sometimes achieved through the use of excessively long and complicated privacy policy agreements with clauses granting the organisation such rights. This is a cause for concern as the layman might not understand the complex terms in these legal documents, coupled with the fact that studies have shown that most people don't even read documents in detail before agreeing or giving their consent (Berreby, 2017). However, the PDPA protects individuals from such "rogue" privacy policy agreements, stating that "organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances" (PDPC, 2018).

The PDPA is beneficial as it increases an individual's trust in organisations that process their personal data and protects individuals from falling victim to unreasonable terms of service. However, we must also acknowledge the limitations and shortfalls of the PDPA.

Firstly, although enforcement action could be taken against foreign organisations, it is hard to perform the enforcement itself due to the consideration of international and regional laws. Moreover, it may also be hard to identify individuals or organisations behind phishing sites. Not much can be done to curb the proliferation of phishing sites, apart from educating the public and blocking suspected sites.

Major Stakeholder in Personal Data Security

In spite of all the security measures taken on a personal, organisational and governmental scale, one might still be at risk of losing their personal data. This can occur due to an oversight during the production process of a gadget used by the masses.

For example, Lenovo inadvertently compromised the security of all of its users when it pre-installed an adware on their devices (Wakefield, 2015). The adware gave users a false sense of security as although their web browsers displayed valid SSL certificates, these were actually issued by the adware, *Superfish*, not from reputable certificate authorities. Hence, when hackers managed to crack the *Superfish* certificate, it exposed anyone with *Superfish* installed to a man-in-the-middle attack (Brandom, 2015). Despite Lenovo providing assistance to remove the adware and facing a financial penalty after this security concern was discovered, the damage had already been done (Brandom, 2017). It is unclear exactly what or how much of an affected person's personal data may have been compromised.

In a more recent example, a banking trojan was found to have been pre-installed in certain Android phones (Cimpanu, 2018). The trojan, *Triada*, is able to gain root access on an affected device, making it impossible to remove even with a factory reset. This was again due to an oversight by the phone manufacturing companies which failed to verify the integrity of their software partners (Cimpanu, 2018).

With just two simple examples, we can clearly see how the decisions made by companies of mass market gadgets actually play an indirect role in determining one's security of personal data. Such misinformed decisions usually slip through the detection of government regulators and most layman users of tech gadgets. While it is unclear whether any of these companies received any financial incentives to make such decisions, they should be morally bound to ensure the security of their products.

Conclusion

By demonstrating how personal data could be misused, it is evident that the consequences of not protecting it are quite severe and commonly result in financial losses. However, we do recognise that there are occasions where the sharing of personal data is essential and beneficial for individuals. We feel that individuals do recognise the risks of not protecting their data but are not taking sufficient measures to protect their own data and rely heavily on organisations or governments to protect their data. This could have been due to a lack of knowledge on how to protect themselves, underestimating the potential dangers of exposing their personal data or are unwilling to take the extra effort to ensure the security of their data.

In addition, we have reviewed on the rationale and possible methods in protecting personal data from different stakeholders — individuals, organisations and governments. While we agree that all three groups are required to share the responsibility and step up to protect personal data, we have identified organisations as the major stakeholder. While individuals may take reasonable steps to ensure the security of their personal data, few have the technical capability to check if brand new products have been compromised. Similarly for governments, while there are regulatory bodies to monitor the release of new products, they simply do not have the capacity to do a thorough analysis of every single product entering the market for security flaws or audit every single organisation.

As organisations are typically the initiator in the collection of consumers' personal data or producer of products used by many, they should take the lead in personal data protection. Thus, they should be morally bound to safeguard consumers’ personal data in order to help curtail cyber crime.

References

Ackerman, S., & Thielman, S. (2016, February 9). US intelligence chief: We might use the internet of things to spy on you. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Agrawal, R., Srikant, R. (2000). Privacy-preserving data mining. *SIGMOD '00 Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, 439-450. https://doi.org/10.1145/342009.335438

Aw, C. W. (2017, December 27). Drugs, weapons and credit card information for sale online: Experts warn about growing threat of dark Web. *The Straits Times*. Retrieved from http://www.straitstimes.com/singapore/drugs-weapons-and-credit-card-information-for-sale-online-experts-warn-about-growing

Banyal R. K., Jain, P., & Jain, V. K. (2013) Multi-factor Authentication Framework for Cloud Computing. *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*. 105-110. https://doi.org/10.1109/CIMSim.2013.25

Bell, L., Merriman, C. (2015) Best IoT devices for the connected home. *The Inquirer*. Retrieved from https://www.theinquirer.net/inquirer/feature/2421020/best-iot-devices-for-the-connected-home

Berreby, D. (2017, March 3). Click to agree with what? No one reads terms of service, studies confirm. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

Brandom, R. (2015, February 19). The Superfish certificate has been cracked, exposing Lenovo users to attack. *The Verge*. Retrieved from https://www.theverge.com/2015/2/19/8069127/superfish-password-certificate-cracked-lenovo

Brandom, R. (2017, September 6). Lenovo pays $3.5 million for preinstalling Superfish adware. *The Verge*. Retrieved from https://www.theverge.com/2017/9/6/16261988/lenovo-adware-superfish-settlement-fine-state-ag

Cimpanu, C. (2018, March 2). Banking Trojan Found in Over 40 Models of Low-Cost Android Smartphones. *Bleeping Computer*. Retrieved from https://www.bleepingcomputer.com/news/security/banking-trojan-found-in-over-40-models-of-low-cost-android-smartphones/

Cheok, J. (2016, April 22). First batch of personal data offenders slapped with fines, warnings. *The Business Times*. Retrieved from http://www.businesstimes.com.sg/government-economy/first-batch-of-personal-data-offenders-slapped-with-fines-warnings

DBS. (n.d.). *Money Safe Guarantee*. Retrieved from https://www.dbs.com.sg/personal/deposits/bank-with-ease/money-safe-guarantee

DBS. (n.d.). *Protecting Yourself Online*. Retrieved from https://www.dbs.com.sg/personal/deposits/bank-with-ease/protecting-yourself-online

D'Onfro, J. (2018, March 22). Mark Zuckerberg says he's 'really sorry' about the company's data scandal. *CNBC*. Retrieved from https://www.cnbc.com/2018/03/21/mark-zuckerberg-addressing-cambridge-analytica-data-scandal-on-cnn.html

EU GDPR. (n.d.). *Home Page of EU GDPR*. Retrieved from https://www.eugdpr.org/

Facebook. (2018). *I don't know why someone received an invitation to join Facebook from me*. Retrieved from https://www.facebook.com/help/android-app/347585398628484?helpref=uf_permalink

Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Retrieved from https://www.gartner.com/newsroom/id/3598917

Google. (2018). *Manage or delete your Location History*. Retrieved from https://support.google.com/accounts/answer/3118687?hl=en

Knieff, B. (2017, July). *2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From*. (p. 7) Retrieved from https://www.aciworldwide.com/-/media/files/collateral/trends/2016-global-consumer-card-fraud-where-card-fraud-is-coming-from.pdf

KPMG, Singapore. (2016). *Companies that fail to see privacy as a business priority risk crossing the creepy line*. Retrieved from https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

O'Neill, M. (2018, February 22). Hackers stole more Social Security numbers than credit card numbers last year - looting $16.8 billion. *Daily Mail Online*. Retrieved from http://www.dailymail.co.uk/sciencetech/article-5423941/Hackers-stole-Social-Security-numbers-2017.html

Personal Data Protection Commission, Singapore. (2018, February 21). *Personal Data Protection Act Overview*. Retrieved from https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

Personal Data Protection Commission, Singapore. (2018, February 21). *Personal Data Protection Breaches*. Retrieved from https://www.pdpc.gov.sg/Organisations/Enforcement-Matters/Personal-Data-Protection-Breaches

Pinola, M. (2017, November 3). *What Are WEP, WPA, and WPA2? Which Is Best?*. Retrieved from https://www.lifewire.com/what-are-wep-wpa-and-wpa2-which-is-best-2377353

Provazza, A. (2017, May 26). Artificial Intelligence data privacy issues on the rise. *Searchmobilecomputing*. Retrieved from http://searchmobilecomputing.techtarget.com/news/450419686/Artificial-intelligence-data-privacy-issues-on-the-rise

Roderick, L. (2016, October 6). Fitbit on how it looks to integrate more deeply into healthcare. *Marketing Week*. Retrieved from https://www.marketingweek.com/2016/10/06/fitbit-on-how-it-looks-to-integrate-more-deeply-into-healthcare/

Rolls, Jon. (2008, October). How to prevent internal breaches. *Computer Weekly*. Retrieved from https://www.computerweekly.com/opinion/How-to-prevent-internal-data-breaches

Sterling, G. (2017, August 23). *FTC-Uber data settlement subjects company to privacy audits for next 20 years*. Retrieved from https://marketingland.com/ftc-uber-data-settlement-subjects-company-privacy-audits-next-20-years-221970

Wakefield, J. (2015, February 19). Lenovo taken to task over 'malicious' adware. *BBC*. Retrieved from http://www.bbc.com/news/technology-31533028

Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y., & Chen, Z. (2009). How much can behavioral targeting help online advertising? *Proceedings of the 18th International Conference on World Wide Web - WWW 09*. 261-270. https://doi.org/10.1145/1526709.1526745