Group 10-17

FUTURE TRENDS REPORT

Community studied:
People who utilise social media

Step 1: Identify Challenges

Interviewees during our survey:

1. Come from different ages between 13-45
2. We chose these groups of people because they are the ones directly affected by this issue and by conducting our survey with responses from different age groups, we are able to gain better insights into this issue.
3. These people tend to spend lots of time on their mobile devices and social media is something very closely connected to mobile devices.

Challenge #1:

Observation: Based on our survey. almost all of the interviewees said that they frequently post or utilised social media. Most also state that they feel their data is not safe online because social media platforms collect their data and sell it to malicious 3rd party apps.

With the rapid increase in the number of social media platforms users, social media platforms are able to collect more and more data about you and maybe know more about you than you know about yourself. Users data are being sold by social media platforms to unknown 3rd party software which may be ill-using our data for their own personal gains. For example, these third party companies might take your email address and password in which you had released to Facebook and Google without knowing about it, and pretend to be you and send out emails. Other than this, they might use you personal data for ransom and demand you to pay them amounts of money if not they would publicly disclose these private information.

Research:

"We have to seriously challenge the claim by Facebook that they are not selling user data. They may not be letting people take it away by the bucket load, but they do reward companies with access to data that others are denied, if they place a high value on the business they do together. This is just another form of selling."

Damian Collins MP, chair of the UK Parliament's Digital, Culture, Media and Sport Committee commented.

From this research has shown, we can see that big social platforms may be secretly selling, or “rewarding” to other companies that can access users’ data. Which is very dangerous as if the government really believed what they “claim”, then no action would be taken, causing us users to lose more and more personal data to those companies. Thus more and more hacking of accounts would happen.

Facebook's data-sharing deals exposed. (2019). Retrieved 4 August 2019, from https://www.bbc.com/news/technology-46618582

In the wholesale market for personal data, companies trade or use our information to target advertising. The average value of an active user to Facebook, based on its most recent earnings release, reached about $2 per month in the third quarter of 2018; in the U.S. and Canada, it was about $9.20. The more precisely the data can be targeted to a user, the more that user is worth.

Bloomberg - Are you a robot?. (2019). Retrieved 4 August 2019, from https://www.bloomberg.com/opinion/articles/2019-01-31/facebook-users-should-be-free-to-sell-their-personal-data

Although Facebook and large social media companies fiercely deny that they do not sell their users data to 3rd party apps, it seems that many people, even politicians feel that in fact, they actually do. In the eyes of the giant social media companies, we users are no more than just tools that they use to gather data and gain economic profits.

Challenge #2:

Observation: Conducted a survey with 70 responses and quite a few respondents stated that they would use either a weak password or use the same password for their social media and other accounts. **Which makes them vulnerable to being hacked.**

Due to the 4th Industrial Revolution, technology is improving rapidly. Hackers being able to decode passwords easier and quicker with new software. Just by hacking one of your account's passwords, they will be able to gain access to all of your accounts, including your social media, which contains the most amount of personal data.

Research: According to the Public Awareness Survey conducted in 2017 by the CSA, Cyber Security Agency of Singapore, about 1 in 3

respondents continue to store their passwords on their computer and use the same password for work and personal accounts. Also, over 6 in 10 respondents do not change their passwords regularly, or only did so when the system prompted them to do so

CSA's Public Awareness Survey in 2017 Reveals Signs of Improvement in Cybersecurity Practices. (2019). Retrieved from https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2017

By using the same password for numerous accounts, once hackers are able to access one of your accounts, they would be able to hack all of your accounts with one of your passwords. Thus all your personal data will be stolen in one fell swoop and can result in identity theft, blackmailing for personal financial gain or stealing of infrastructure where they might use your cloud-sharing subscriptions to host their apps without needing to pay.

Challenge #3:

Observation: Almost all of respondents stated that they would connect to "Terms and Conditions" of software that they utilise **without looking through the terms and conditions.**

For example, when they create a Facebook or Instagram account, they would not look through the privacy policy and simply agree to it.

People are not aware of the present dangers due to their negligence by accepting the Terms and Conditions without reading them. By accepting the privacy policy, you may not know exactly what kind of data they are

collecting about you and who can see your data. This may lead to their data being stolen (such as browsing data).

Research:

1. A Deloitte survey of 2,000 consumers in the U.S found that 91% of people consent to legal terms and services conditions without reading them. For younger people, ages 18-34 the rate is even higher with 97% agreeing to conditions before reading.

Cakebread, C. (2017). *You're not alone, no one reads terms of service agreements*. [online] Business Insider. Available at: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?IR=T [Accessed 4 Aug. 2019].

This shows how vulnerable people are to having their data farmed when the language of the T&C is too complex and long-winded for most, and apparently, consumers are willing to accept that the worst most companies will do is sell their name and email to a third party that wants to advertise to them.

Challenge #4:

Observation: Amongst our interviewees, many of them also expressed concern about the possession and concentration of data amongst leading tech firms like Facebook and Google.
This sharply increases the risk of all the data that they have farmed from millions of people to be all lost in one hacking. This vulnerability could result in widespread alarm and confusion as all the hackers need to do to be able to access millions of people's data is just to hack the Facebook server where they store all their users data. This makes their job much easier as they do not need to constantly try to gain access to multiple databases

Research:

According to Yuval Noah Harari, in a TED talk about personal data, he stated that “Too much data is being concentrated in the hands of the government or of a small elite.”, and that “it was simply inefficient to try and concentrate too much data and too much power in one place.”

Harari, Y. (2018). Why fascism is so tempting -- and how your data could power it. Retrieved 4 August 2019, from https://www.ted.com/talks/yuval_noah_harari_why_fascism_is_so_tempting_and_how_your_data_could_power_it?language=en

This shows us the importance of not concentrating all our data in one location, which makes it extra vulnerable to being hacked in one fell swoop. These leading companies also have no security benchmarks to comply to, and can protect their data in whatever ways they deem acceptable.

Challenge #5:

Observation: According to our survey, some people expressed concern that not enough is done by the Government to regulate the flow of data throughout social media platforms such as Facebook from selling our data to 3rd party apps for their own economic benefits.

The lack of regulation/regulatory frameworks is that which has caused Facebook to continue to engage in covert operations that farm users' data without them knowing.. Even though the issue has only come to light in recent years, most governments just talk and negotiate with Facebook but end up taking no action against their unknown distribution to other 3rd party apps of our personal data.(distribution of our personal information without us knowing in whose hands does the information land)Thus this issue has not improved or changed for the better, which is worrying for us users.

Research:

According to https://www.bbc.co.uk, a recent leak of Facebook's data-sharing deals showed that:

1. Microsoft's Bing search engine was able to see the names of "virtually all" Facebook users' friends without those friends' consent in order to personalise the results it showed
2. The music-streaming service Pandora and film review platform Rotten Tomatoes also had access to friends' information in order to customise their results
3. Apple devices could access the contact numbers and calendar entries of users even if they had disabled all sharing in their Facebook settings. Moreover, it said Apple's devices did not need to alert users to the fact they were seeking data from Facebook
4. Netflix, Spotify and the Royal Bank of Canada were able to read, write and delete users' private messages and see all participants on a chat thread

5. Russian search provider Yandex was allowed to index users' identities from public pages and posts to improve its search results after Facebook stopped other applicants from continuing the activity
6. Yahoo could view live feeds of friends' posts
7. Sony, Microsoft and Amazon could access members' email addresses via their friends
8. Blackberry and Huawei were among companies that could pull Facebook's data to power their own social media apps

BBC News. (2018). Facebook's data-sharing deals exposed. [online] Available at: https://www.bbc.co.uk/news/technology-46618582 [Accessed 4 Aug. 2019].

If there is a proper regulatory framework in place that penalises social media platforms for “selling” our data, such activities would not have taken place in the first place.

STEP 2: UNDERLYING PROBLEM

Underlying problem we have formed:

Given that there is no way for one to find out what social media platform companies like Facebook and Google do with the data that they harvest from your digital footprint, such as selling it to an unknown third-party companies which might abuse it, how might we better protect Singapore users of social media from such data abuse so that the risk of identity theft, data ransom, can be reduced.

STEP 3: Crafting Solution Ideas

Solution 1:

We, the Ministry of Data Protection, will form a data monitoring force which will monitor the flow of data and what it is used for within large social media platforms such as Facebook and Google to prevent the distribution of data to third parties online who can manipulate and abuse it to commit identity theft or worse(for example, using someone else's identity to commit crimes.)

For example, this force will constantly monitor how Facebook in Singapore obtains personal data and uses or distribute it. If any data privacy issues were to surface that are in fact, not complying to the Personal Data Protection Plan (PDPA),
For example, if the data protection force finds out that Facebook is secretly selling data to dubious companies that have not been legalised for extra revenue or these companies discloses personal data without the consent of the user, **the government will be notified and the leak of these data will be prevented. Regular data protection compliance checks will be conducted on Facebook's servers to ensure that their massive amounts of farmed data is securely protected against hackers.**

Research:
According to *https://www.todayonline.com*, The importance of digital awareness has never been higher and the amount of hackers and scams in the present world is on the rise. This emphasises the importance of the protection force which can fish out threats that might be overlooked by the public.

Digital defence key to success of S'pore's Smart Nation drive: Iswaran. (2019). Retrieved 30 July 2019, from https://www.todayonline.com/singapore/digital-defence-key-success-spores-smart-nation-drive-iswaran

Solution 2:

We, the Ministry of Data Protection, will come up with a firewall that must be present in all electronic devices in Singapore and this firewall will block off the release of personal and confidential data (such as: NRIC, Credit Card number) to servers such as Facebook and other social media platforms.

We can never completely prevent that social media platforms from collecting data and selling it to 3rd party apps. But the important thing is that our important personal data (see above) must never end up in the hands of social media companies and get "sold". With this firewall, the amount of personal data available for 3rd party collection will be minimized.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

Services, P. (2019). What Is a Firewall?. Retrieved 4 August 2019, from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

A firewall is ultimately have flaws and it is only a matter of time before social media companies find a way to bypass the firewall and gain access to our personal information. However, if they want to find a way to bypass this firewall, they would need the help of hackers to do so. If the masses were to find out that large social media companies were resorting to such measures to gain our personal data, there would definitely be an outrage and social media companies will lose their credibility and many would stop using their platform. This would ultimately result in major economic losses. So, if the major social media companies were to try to bypass this firewall, it would do them no good.

Solution 3:

We, the Ministry of Data Protection, will come up with an alternative social media platform to Facebook and Instagram for Singaporeans only.
This social media platform will be introduced and advertised to give an alternative to the current platforms such as Instagram, Facebook, etc. and these platforms will be monitored closely by the Ministry of Data Protection.

It also promises that no data of yours will be shared to those whom you do not know and allow and will be kept private at all costs. Thus, users will be able to use this platform safely, knowing that their data will be 100% secure. Since it is a Government-run software, it will be non-profit and thus would not need to farm data to make profits.

Google knows where you've been, everything you've ever searched – and deleted, has an advertisement profile of you, knows all the apps you use, all of your YouTube history, and the data Google has on you can fill millions of Word documents.
Facebook knows everything from your stickers to your login location, can access your webcam and microphone, and basically also everything Google knows of you too.
Curran, D. (2019). Are you ready? This is all the data Facebook and Google have on you | Dylan Curran. Retrieved 4 August 2019, from https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

This shows the dire consequences of using these unregulated softwares and applications. Using the government's new completely private social media platform, none of your personal data would be divulged to third-parties, providing its users with a greater sense of security when surfing the internet.

Our platform which we will create will have many special features. To make sure that our platform engages the public, we will firstly compile all the features of various successful social media platforms and implement them into our platform. However, our social media has this special feature...you are able to meet your friends in Virtual Reality and speak to them! All you need is a VR headset!
Also, our platform will come in many different languages to cater to the different races and nationalities in Singapore. We will also have constant updates and bug fixes so that people will enjoy using our app and continue using it as an alternative for global social media platforms.

Solution 4:

We, the Ministry of Data Protection, will create a reward-system website with quizzes and puzzles that educate the public about the risks of using social media. Students must complete at least 10 quizzes a year as a compulsory digital security curriculum and the top scorers will be rewarded. These quizzes will be fun and creative, which will also pique the children's interest. From this, students can also become advocates for the cause after they learn and further promote awareness for the risks of using social media.

1. According to a research paper done by *Dr. Jennifer Hillman* on "The Impact of Online Quizzes on Student Engagement and Learning",
   The use of online, out of class quizzes allowed the instructor to have significantly more time for in-class active learning activities (e.g., debates, role plays, small group activities), and generated more lively and in-depth class discussions because students typically read the material before class in order to perform well on the online quiz. Students were very positive about the online quizzes in terms of ease of use,

ability to learn course material in a timely, measured fashion, preparation for both class and comprehensive exams, and to improve their course grade, as well.

Hillman, J. (2012). The Impact of Online Quizzes on Student Engagement and Learning [Ebook] (p. 5). Retrieved from https://berks.psu.edu/sites/berks/files/campus/Hillman_TLI_report.pdf

2. **According to the Guardian,**
   "You could argue that some of the most important changes in the world, such as the end of the slave trade or votes for women, were achieved through advocacy. Knowing how to do it well is crucial for people who want to shape our world for the better."

Effective advocacy 101: how to bring about change in five steps. (2019). Retrieved 5 August 2019, fromhttps://www.theguardian.com/global-development-professionals-network/2016/jan/12/effective-advocacy-101-how-to-bring-about-change-in-five-steps

This shows the great results that e-learning brings about and how impactful advocacy is in changing and impacting the future and if we are able to have effective advocacy through the senior students, this will allow our younger generation to grow up to become responsible users of social media and will be able to understand the risks of posting and utilising social media under the strong influence of their seniors.
Also, through advocacy developed through a heightened sense of interest, the awareness of this issue will definitely increase and more and more people will be made aware of this issue and understand the risks of posting and utilising social media.

Solution 5:

We, the Ministry of Data Protection, will enforce an "allowance" on large social media companies with great amounts of personal data in which there is a limit imposed on the number of people's data that Facebook can collect.

We are well aware that data is the main source of income for these social media platforms, thus we will set a reasonable limit. where there is not a major impact on the profits of the companies, yet, not too much of personal information is disclosed.
According to Statista, currently 4.4 million in Singapore use social media platforms.

Number of social network users in Singapore 2023 | Statista. (2019). Retrieved 5 August 2019, from https://www.statista.com/statistics/489234/number-of-social-network-users-in-singapore/

If we were to set a limit on how many people's data Facebook can harvest while not losing out on profit, we would propose 75%, which would be 3.3 million people. The reason why we chose this number is because another source of revenue for these social media platforms would be advertising and the price of advertising ranges from $850 to $2750 per month. If the social media platforms have 1,295 companies advertising at the minimum price, they would already be able to make up for the 1.1 million. In contrast, if all their customers were to purchase the maximum price of advertising, social media platforms would only need 400 customers to make up for the money lost. Thus, it would still be relatively easy for the social media companies to get profits if their data farming gets cut by 25%.

How Much Does Social Media Advertising Cost in 2019? | WebFX. (2019). Retrieved 6 August 2019, from https://www.webfx.com/how-much-does-social-media-advertising-cost.html

This will greatly reduce the amount of data that is collected by social media platforms considering that a large percentage of

Singaporeans use social media platforms.

Research:
Taking into consideration the fact that one of the biggest risks to people who use the services of both the public and private sector is the possibility of a data breach, and the fact that data breaches have been increasing consistently both in frequency and intensity, now would be a good time to begin pressuring the companies we use to either catalog less of our data or at least improve their security practices.
Leiva-Gomez, M. (2019). Where Do We Draw the Limit on Data Collection?.Retrieved 4 August 2019, from https://www.maketecheasier.com/draw-limit-on-data-collection/

STEP 4a: Selecting Criteria

1. Which Solution will be **easiest to implement** for us

   Which solution can be implemented with the least resources so that the cost will not be too high

2. Which Solution will **make the most impact in the long run**

   Decide the sustainability of our solution and create an impact that will last for an extended period of time.

3. Which Solution will be with the **highest demand**

   Determine if our solution actually has people who want to use it in the first place, before we start developing it. This demand also affects whether the public will readily accept and adopt the solution.

4. Which Solution with **more impact in a shorter amount of time**

   So that we are able to determine if the solution wields faster results and has a greater impact but not very long lasting effects.

5. Which Solution is **more original**

   So that there would not be so many duplicate ideas, which may result in clashes and also our solution not being able to stand out amongst the other solutions on the internet.

STEP 4b: DECISION MAKING-MATRIX

Criteria	Easiest to implement (Weightage:5)	Most impact in long run (Weightage:4)	Highest Demand (Weightage: 3)	Most impact in shortest time (Weightage: 2)	Most original (Weightage :1)	Total
SOL 1	20	20	9	10	4	63
SOL 2	15	16	15	6	3	55
SOL 3	10	8	12	2	5	37
SOL 4	25	4	3	8	1	41
SOL 5	5	12	6	4	2	29

We have chosen Solution 1:

We, the Ministry of Data Protection, will form a data monitoring force

STEP 5: ACTION PLAN

Action plan derived from solution 1:

This data protection force will work in the Ministry of Data Protection office. We will make sure we gather the brightest prospects in the cyber community and form this force. This force will make sure that the flow of Singaporeans data on social media platforms will be compliant to the PDPA and make sure no data will be sold to dubious 3rd party apps who have not been legalised for extra revenue.

This protection force will be assembled as quickly as possible and should be fully functional and in place by 2030 and the service they provide will be free.

Although the costs of setting this task force up may be large,the Government will definitely have the financial capabilities to do so. Furthermore, the impact this force will have on the community and the future will definitely outweigh the huge costs. And us being the Government, we must always put our people in front of ourselves and do what is best to serve them.

This force will begin its setting-up in 2020 and will be fully functional and in place 2030.

Implementation Timeline

- 2020: Negotiations with Facebook and social media platforms and parliament to allow this force to function. This should be done in 5 years.
- 2025: Parliament agrees to implement the Data Protection Force to help better protect Singaporeans data.
- 2026: Begin the search for experienced technicians and programmers
- 2027: We will officially form the Data Protection Force and we will begin operations on a small scale as a trial run to see if we can obtain results
- 2028: Feedback from social media users on whether they feel change when utilising social media.
- 2029: Based on the feedback we receive, we will improve our services and infrastructure to better cater to the needs of social media users.
- 2030: Our task force will begin operating full-time, protecting Singapore citizens data.

Addressing the Key Verb Phrase

Given that our key verb phrase "how might we better protect Singapore users of social media from such data abuse", our action plan and solution address this since the data protection force will work behind the scenes to help monitor the flow of Singaporean's personal data and prevent the misuse of our data. (such as disclosing personal info without our consent) This will definitely better protect the data of Singaporeans who use social media regularly.

Resistors and Supporters

We believe that the social media users in Singapore will generally support this force because having this force would allow them to be safer online and it would only do them good to have this task force around.
However, we believe that the resistors will be the social media companies as it will seem that they are always being scrutinised at and it may affect their economic profits by not being able to sell as much data.

Potential Challenges

1. Making the parliament social media platform companies to agree to implement this force
2. Finding good employees with experience and talent
3. It may be hard to find constructive feedback from the public

Solutions

1. If we raise the awareness of this issue amongst the public, and this issue becomes a pressing concern, the Government will definitely try to solve this issue raised by the public.

This makes it highly likely for the parliament to agree to our solution. In order to raise awareness, talks and workshops about how our data is used on social media platforms can be organised to raise awareness for this issue.

2. If we offer good pay with exclusive benefits to employees, more people with experience and talent will definitely be willing to take up this job,

solving the problem.

3. Some members of the public when asked to give feedback, some are not even aware of things while some just fool around. We can reduce such things from happening by setting a serious tone in the feedback form and also let the public know that these feedback will allow them to be better protected, have a better experience online and they should take it seriously.

Research:

1. According to "*On Privacy and Security in Social Media – A Comprehensive Study*" done by *Kumar N, S., K, S., & K, D,* "Facebook could plainly express that they could give no assurances with respect to the privacy of their information, and that if clients make their profiles open, all data contained in that may be seen by occupation questioners and school chairmen."

   "Late research has investigated the relationship between the online revelation of individual data and privacy concerns and the high hazard identified with online ruptures of protection".

   This shows that Facebook itself knows that their ways of handling their users data does not definitely guarantee their users privacy of their information and so, something must be done by others to ensure that our data will not end up in the wrong hands of 3rd parties who can misuse our data.

2. Peter Wells, Head of Policy at the Open Data Institute said: "There's no inspection regime either by Facebook or by government: both could play that kind of role, though they'd be doing it for different purposes."

   After Cambridge Analytica, here's what government can do to protect data | Apolitical. (2019). Retrieved 6 August 2019, from https://apolitical.co/solution_article/after-cambridge-analytica-heres-what-government-can-do-to-protect-data/

   This shows that no inspection regime has been taken by the Government on this pressing issue on data privacy. Others out there in the world, including experts feel that an inspection regime is infinitely important and must be done and in place as soon as possible.

Citations:

- *Facebook's data-sharing deals exposed. (2019). Retrieved 4 August 2019, from https://www.bbc.com/news/technology-46618582*
- *Bloomberg - Are you a robot?. (2019). Retrieved 4 August 2019, from https://www.bloomberg.com/opinion/articles/2019-01-31/facebook-users-should-be-free-to-sell-their-personal-data*
- *CSA's Public Awareness Survey in 2017 Reveals Signs of Improvement in Cybersecurity Practices. (2019). Retrieved from https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2017*
- *Cakebread, C. (2017). You're not alone, no one reads terms of service agreements. [online] Business Insider. Available at: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?IR=T [Accessed 4 Aug. 2019].*
- *Harari, Y. (2018). Why fascism is so tempting -- and how your data could power it. Retrieved 4 August 2019, from https://www.ted.com/talks/yuval_noah_harari_why_fascism_is_so_tempting_and_how_your_data_could_power_it?language=en*
- *BBC News. (2018). Facebook's data-sharing deals exposed. [online] Available at: https://www.bbc.co.uk/news/technology-46618582 [Accessed 4 Aug. 2019].*
- *Digital defence key to success of S'pore's Smart Nation drive: Iswaran. (2019). Retrieved 30 July 2019, from https://www.todayonline.com/singapore/digital-defence-key-success-spores-smart-nation-drive-iswaran*
- *Services, P. (2019). What Is a Firewall?. Retrieved 4 August 2019, from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html*
- *Curran, D. (2019). Are you ready? This is all the data Facebook and Google have on you | Dylan Curran. Retrieved 4 August 2019, from https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy*
- *Effective advocacy 101: how to bring about change in five steps. (2019). Retrieved 5 August 2019, fromhttps://www.theguardian.com/global-development-professionals-network/2016/jan/12/effective-advocacy-101-how-to-bring-about-change-in-five-steps*
- *Hillman, J. (2012). The Impact of Online Quizzes on Student Engagement and Learning [Ebook] (p. 5). Retrieved from https://berks.psu.edu/sites/berks/files/campus/Hillman_TLI_report.pdf*

- *Number of social network users in Singapore 2023 | Statista. (2019). Retrieved 5 August 2019, from https://www.statista.com/statistics/489234/number-of-social-network-users-in-singapore/*
- *How Much Does Social Media Advertising Cost in 2019? | WebFX. (2019). Retrieved 6 August 2019, from https://www.webfx.com/how-much-does-social-media-advertising-cost.html*
- *Leiva-Gomez, M. (2019). Where Do We Draw the Limit on Data Collection?.Retrieved 4 August 2019, from https://www.maketecheasier.com/draw-limit-on-data-collection/*
- *Kumar N, S., K, S., & K, D. (2015). On Privacy and Security in Social Media – A Comprehensive Study [Ebook]. Science Direct. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050916000211*
- *After Cambridge Analytica, here's what government can do to protect data | Apolitical. (2019). Retrieved 6 August 2019, from https://apolitical.co/solution_article/after-cambridge-analytica-heres-what-government-can-do-to-protect-data/*