Group ID: 10-34

Future Trends Report
Based on Analysis of the Team's Chosen Community / Organisation in Mid-Term and Final Evaluation

Organisation Studied: Paypal

STEP 1. Identify Challenges

Read the Future Scene carefully and generate ideas for challenges, concerns, and possible related problems. Choose the 5 most important challenges and write them in the space provided. Include applicable research with appropriate in-text citations.

Challenge #1:

Based on our interview, online payment companies obtain a lot of data from its consumers, however they are unable to push out too many relevant and enticing offers to consumers, as it might be an overdose for consumers and make them feel uncomfortable. ***(observation)***

This might result in online payment companies being unable to find a balance between an excessive number of offers and a deficit amount. If an excessive amount of offers are directed at consumers, they might reject the push notifications or delete the app completely to avoid the spam. If they do not send out enough offers, the customers may be compelled to go to another online payment company that pushes out more enticing deals more often. Online payment companies have to strike a balance between sending out too many offers, so as to not deter customers away from their company, and sending out too little offers. ***(why)***

"Data integration is already a huge challenge for email marketers, but in the next few years it is going to become the issue that separates world-class marketing organizations from the rest of the pack," says Loren McDonald, Marketing Evangelist at IBM Watson Marketing. Data integration refers to combining data residing in different sources and providing users with a unified view of them, a process which becomes significant in both commercial and scientific domains. It is imperative that companies learn how to incorporate data into their marketing strategy such that advertising is most well targeted at consumers. ***(research)***

Challenge #2:

Based on our interview, consumers are wary of privacy issues, especially in Singapore, where people prefer physical form of payment over digital payment avenues like Paypal due to privacy concerns. ***(observation)***

Consumers may be unwilling to provide personal information that these online payment avenues require to be used, which might result in less people using the system, reducing business from consumers and clients. Most consumers feel that they have little to no control over their personal data and some of them feel that companies are willing to profit at the expense of their consumers' data. Furthermore, some consumers feel that the potential risks they face because of data collection by companies may outweigh the benefits presented in using online payment systems and hence would choose not to use these online payment systems. ***(why)***

A study by Paypal in 2017 revealed that 90% of Singaporeans preferred cash payments and only 3% of consumers used digital payments regularly. This could have been a result of a lack of transparency between companies and consumers, as consumers do not know how much of their data is being accessed. According to Pew Research Centre, 62% of respondents feel that it is not possible to go through everyday life without their data being collected by companies. This lack of trust could be detrimental to the usage of the company's products. If consumers do not have enough trust in the company, they will be unwilling to switch to online payment systems. ***(research)***

Challenge #3:

Based on our interview, online payment systems' main mode of notification of offers and opportunities is through email, however this may not be the main mode of communication in many countries, with email being used much more commonly in more serious settings like formal proposals. **(*observation*)**

Much like many other companies, online payment systems mainly rely on email to push out offers and opportunities. However, email, in recent years, has proven to be less and less effective in the context of advertising; with many more methods of communication online these few years, it is not a surprise that the use of email has declined. This results in online payment systems not being able to effectively push out the relevant offers and opportunities to its consumers and will in turn leave them with less business from its clients as well. **(*why*)**

According to Google trends, the usage of gmail peaked in 2014 but has been on a steady decline ever since. With such a decline in the usage of email, it is no surprise that such a mode of communication may not be the best for communication with customers. A study by Litmus highlighted the potential challenges met by email marketers; including but not limited to : Poor coordination between other departments and channels, Insufficient staffing, as well as the decline in usage of gmail over the years due to other applications being used such as Telegram and Whatsapp. **(*research*)**

Challenge #4:

Based on our interview, some countries may be extremely sensitive to obtaining data from its consumers. ***(observation)***

This results in online payment companies having to use inbound methods to gain consumers' attention, such as subtly promoting their system and providing a call line for interested consumers. This is much more ineffective compared to outbound methods, such as pushing out offers or advertising. This reduces the efficiency of their businesses, which will affect their volume of sales. ***(why)***

Our interviewee telsl us that one such example is Japan, where the government restricts companies such as Paypal from obtaining its citizens' data so openly, resulting in companies having to use other methods to obtain data from users such as subtle pop up advertisements that consumers can easily ignore. This method of advertising pales in comparison to outbound

methods of advertisements where advertisers are able to openly communicate with the consumers through online services such as Gmail, where users are unable to avoid the deals and offers presented by the online payment systems. ***(research)***

Challenge #5:

Based on the interview, online payment systems face the possibility of data overload, which could lead to crashes, with too much data and transactions. ***(observation)***

With the development of technology and increased popularity of online payment systems, it is inevitable that the number of users will start going up, and the amount of data stored and transferred will follow suit. Online payment systems can be overloaded with data, dealing with too much information and too many transactions - this could result in these companies being unable to handle this data efficiently, and online payment systems may be unable to cleanse the data they receive as there is too much data to handle. Online payment systems may thus be unable to use information gained from its users properly, and are unable to use this data to improve the company and its service. ***(why)***

According to Fintech, financial services companies have enormous amounts of customer data such as payments done online and customer profile data, but due to their silo, product-oriented organisations, they are not very good in utilizing these rich data sets. This is exacerbated by technological evolutions, which lead to larger amounts of input data that need to be cleansed and processed. New advanced authentication techniques, such as biometric authentication and continuous authentication will also considerably increase the amount of data to be processed in near real-time. ***(research)***

STEP 2. Craft the Underlying Problem

Using the challenges listed in Step 1, identify a problem of major importance to the chosen community / organization in the future. Write your Underlying Problem making sure your question clearly explains the action that will be taken and the desired results/goal of that action.

Incorporating Challenge(s) #2 & #4

Underlying Problem:

Given that online payment systems may misuse the data of its consumers for the use of third party companies, it appears that users may be more susceptible to marketing and targeted advertisements which may influence their decisions. How might we give consumers the free will to choose how their data is managed so that they can be more willing to use these systems in the year 2030 and beyond?

STEP 3. Produce Solution Ideas

Generate solution ideas to the Underlying Problem in Step 2. Choose the 5 most effective solutions and write the elaborated ideas in the space provided. Include applicable research with appropriate in-text citations.

Solution #1:

We, the Ministry of Trade and Industry, will create and mandate the use of an automated system in which online payment systems can ask for approval from a user when using their personal data. This system will make use of biometrics and gaze control technology to ensure that the actual user is giving their approval. This will take place in the year 2030 and beyond. This solution gives users a sense of awareness as they will obtain knowledge about the use of their data. It gives users the free will to authorise the use of their personal data for specific purposes, help reduce misuse of personal data, and biometrics and gaze control ensures that the actual user is authorising the use of their data and prevents impersonation. According to Ubiquity, "*Because one's unique characteristics cannot be stolen, forgotten, duplicated, shared or observed, a biometrics based security system is nearly impossible to fraud*." Biometrics is much more secure as it is based on unique physical characteristics. As compared to current solutions such as internet cookies, where users only consent to the use of their data with a click of a button, it is clearly much more secure.

Solution #2:

We, the Ministry of Trade and Industry, will create an app based on a system which mandates companies to report the user information and data they possess to the government. Users can access this app to understand how much of their personal data companies have. This will be implemented in the year 2030 and beyond. This solution provides free will by allowing users to obtain knowledge on where and how the data is being used, allows users to know if and when they are being targeted and less susceptible to marketing ploys. This application would dissolve the doubts that people have in how their data is being used and make them less paranoid and more comfortable. According to Pew Research Centre, "*76% of adults say they are "not too confident" or "not at all confident" that records of their activity maintained by the online advertisers who place ads on the websites they visit will remain private and secure.*" This application would dissolve the doubts that people have in how their data is being used and make them less paranoid and more comfortable. The role of the government in this solution is to regulate the companies and ensure that companies adhere to the consumers' decisions regarding the usage of their data. This is critical as the system needs to be enforced strictly in order for the solution to work at all - and evidence from recent trials such as Facebook and Cambridge Analytica, where Facebook was fined USD$5B for the misuse of user data, and Google being fined €1.49 billion for breaching the EU's antitrust laws, suggest that companies can in fact be regulated by governments.

Solution #3:

We, the Ministry of Trade and Industry, will create an application that will directly allow its users to track where their data has travelled to and what it has been used for. This will take place in the year 2030 and beyond. This solution will directly report to the users how their data is being used, and gives users the option to enable and disable accessibility to their personal data; allowing users to know how much of their data is being accessed and utilised by companies and gives users the free will to decide whether too much of their personal data is being given up and act if they feel the need to. A good idea of our solution is what Google is doing. Google is already rolling out a new privacy dashboard which makes it easier for users to see what Google knows about them. It allows users to see all of their Google activity, deletes search activity, manages their activity across various Google products like search, Maps, and YouTube, and can be implemented on a large scale system.

Solution #4:

We, the Ministry of Trade and Industry, will create an automated system for government officials to monitor online payment system's use of user's data. Users have the option to receive a report on the use of their data from the government. This will take place in the year 2030 and beyond. This will allow users to know about what online payment systems actually do with their data with this information also being verified by the government and users have the free will to decide if their data is being used appropriately. This solution will largely rely on the government to mandate how data can or cannot be accessed and used. It can be enforced only if consumers and citizens place enough trust in the government to handle their own personal data and ensure that their privacy is

not compromised. As shown in the case studies of Facebook and Google displayed in the research of Solution #2, it can be seen that government regulation is feasible and effective.

Solution #5:

We, the online payment system companies, will give users the option to deny the companies of usage of their personal data. Users can choose to withhold their data from companies and use online payment systems with limited functionality in order to protect their personal data and free will. This will take place in the year 2020 and beyond. This allows the users power over their own data and how they want to handle it with outside parties and they will feel more in control and feel more reassured that they have their own free will over their own personal information. With more reassurance to how their data will be managed, consumers may hence become more willing to use these online payment systems as they will be in control of their own online experience and will trust these companies more, boosting the image of the company as well.

Group ID: 10-34

STEP 4a. Select Criteria

Generate criteria to determine which solution idea does the best job of solving your Underlying Problem and/or addressing the Future Scene situation. Select the 5 most important criteria for measuring solution ideas and write them in the spaces provided.

Criterion #1:
Which solution is the fastest to implement such that consumer autonomy in data privacy may be upheld as soon as possible?

Criterion #2:
Which solution is the most cost efficient for both government and company?

Criterion #3:
Which solution benefits both consumer and company such that the companies gain business while the consumer is protected from data misuse?

Criterion #4:
Which solution works in the long term to ensure the problem of lack of privacy and misuse of data does not occur again?

Criterion #5:
Which solution is the most effective in protecting free will such that the user is able to make a choice on the use of their data?

STEP 4b. Apply Criteria

List the solution ideas from Step 3 on the grid. Use each criterion to rank the solutions on a scale from 1 (poorest) to 5 (best). The weighting for one important criterion may be doubled if necessary.

Step 3 Sol'n #	Solution Idea	Criteria					Total
		1	2	3	4	5	
#1	**Automatic Biometrics System**	**2**	**3**	**5**	**5**	**5**	**20**
#2	App with data usage info	3	4	4	2	3	16
#3	Data Usage Tracking	1	2	1	4	4	14
#4	Government tracking of data usage	4	1	2	3	2	13
#5	Disapproval of use of data	5	5	1	1	1	13

STEP 5. Develop an Action Plan and Evaluate its Feasibility

vcr

Develop your top-scoring solution idea into an Action Plan. Thoroughly explain how the Underlying Problem is solved, how the plan will be implemented, and how the community / organisation will be affected. Explain how this Action Plan is feasible with secondary research consulted, preferably also with primary research (feedback from chosen community / organization)

Action Plan derived from Solution #1, #2 and #5:

The Ministry Of Trade and Industry, with the collaboration of online payment system companies, will create an automated system to allow users to approve specific use of their data, with the data collected from consumers will be stored in a database that MTI has access to.

When the online payment system company wants to use its user's data, an automated message will be sent to the user's email, asking for their approval. The automated email will contain details of what the company is using their data for, such as a customers' purchase history. To approve the use of data, users will have to use biometric iris recognition and gaze control to ensure the identity of the user and each user will have a private and specific gaze movement to approve or disapprove the use of their data. We got our ideas for this action plan from recent studies that have highlighted the potential importance and usefulness of biometrics and gaze control when used for security purposes.

There will be a trial period added to source out problems before the final implementation and also lobby government for funding allocation. As users may have difficulties adapting to the technology, there will also be an option to split up the implementation of the technologies to help users get used to the biotech before gaze control is implemented, as it will take time to be readily available.

Biometrics and gaze control will also be able to effectively reduce human error, which can commonly arise from the use of internet cookies. For the use of these cookies, users simply have to click on a button stating that they have accepted the terms and conditions, allowing for their data to be used by the platform. The nature of this form of asking for consent can result in many problems. One of which is the problem that people usually do not spend their time to read the terms and conditions of these internet cookies and blindly click on the "Accept" button in order to get the pop up out of the way, resulting in unknowing use of their data. On the other hand, biometrics and gaze control is also a much safer option compared to having an app or other methods as it requires a specific physical quality of the user instead of just a simple one click authentication, which makes it impossible for companies to gain access to user's data without their permission.

Secondly, the Ministry of Trade and Industry, will create an app based on a system which mandates companies to report the user information and data they possess to the government.

This system that mandates companies to report user information allows the government to ensure that companies are not abusing their power over the use of consumer data and are only using data when consumers have clearly given permission for them to do so. This provides a sense of responsibility and accountability for companies to be careful with the use of consumer data,

resulting in more security for consumers. Some less confidential parts of this system can also be released to the public, which will allow them to track their data, supplementing the earlier solution of biometrics and gaze control. By integrating these two solutions, users will not only be able to consent or deny data usage, but they can also track their own data to ensure that companies are not misusing their data.

Lastly, the online payment system companies will give users the option to deny the companies of usage of their personal data.

Our system is meant for the customers to fully decide how, where and even *if* their data will be used. With this system, it makes sure that their data will be secure and gives them the liberty on how they want their data to be used, whether it be sold to the companies so that they have more accurate data which allows them to better serve their customers, or to keep the data secure to ensure their own privacy. This also ensures that the company is not working behind their backs to get their data that they want to keep private.

The app created will therefore run based on a database that stores the data of consumers - a database that can be accessed by the government but can only be accessed by the companies if the users use their biometric information to allow for companies to access their data. The system revolves around the consumers and their privacy, with the main priority being the security of consumer data, and this is done so through requiring consumers to acknowledge their data and consent to it being used. All in all, we aim to establish a system that can be accessed by three parties - consumer, company and government. The goal of our action plan is to integrate these three stakeholders such that decisions are made by consumers, with companies adjusting their business and marketing strategies by aligning with consumers' views. The government will only step in to regulate these companies and ensure that the companies do not misuse customer data. Our action plan accomplishes this as biometric confirmation ensures that users have full control over how much of their data companies have access to and what these companies can do with the data. By integrating biometric confirmation and government regulation into the system, the application will allow for easy and convenient access for the users and the government so that security and privacy will be the industry standard for the world of big data in the year 2030 and beyond. Lastly, by allowing consumers to completely withhold their data and reject the use of their personal data, customers are given the freedom to choose to keep everything private, which allows those who are unwilling to trust the application or technology as a whole to have a sense of security. Our action plan therefore helps to tackle the underlying problem by giving consumers as much free will as possible.

With this thorough yet convenient method of consent put in place, not only will it enable consumers to know how and what their data is being used for, but will also ensure security so that only authorised users will be able to consent to the data usage, providing consumers with the choice on how they would like their online experience to be. In the future, biometrics can be integrated into an app on their phone, thus allowing convenient yet secure consent to their data usage.

In order for our system to be successfully implemented, the Ministry Of Trade and Industry has to liaise with online payment system companies on how the system will work. Next, data will be collected from the companies and stored inside MTI's database. A prototype of the system will be made in the next few years followed by a trial and feedback period for the product. Improvements will be made to the system before finally being released in 2030.

Implementation Schedule:

1st: Liaising with companies *(2020-2022)*
2nd: Data Collection *(2022-2024)*
3rd: Prototype *(2024-2026)*
4th: Trial Period *(2026-2027)*
5th: Improvements *(2028-2029)*
6th: Final Implementation (*2030)*

Who will support our action plan?

Target Audience #1: Consumers would support the action plan for the safeguarding and protection of their personal information and data, which gives them a sense of safety both mentally and physically. They will provide support by endorsing and utilising the product to its maximum potential, which is critical to the success of the plan as consumer approval is needed for the plan to be effective in protecting the consumers themselves.

Target Audience #2: The government would support the action plan for the cause of protecting data around the world, and a step in the right direction in the future of ecommerce. Governments can provide support in investing towards the biotechnology industry to develop and allow for the pushing out of these systems.

Target Audience #3: The biotechnology sector would be the brains and hands of this entire process, putting in their efforts and their investment into research and development of these systems. This would happen as the sector would benefit from the action plan in the form of a larger amount of investments in their companies and businesses.

How will this address the KVP?

Our action plan has a singular main purpose of enhancing user privacy and security - and this is done so through all three of the aforementioned incorporated solutions. There is better data security as users can now decide whether they want companies to use their data and what their data should be used for, and this is ensured through biometrics confirmation which is highly secure. Instead of the companies using consumers' data behind their backs, users are given a choice on how they want their data to be managed and will not be as susceptible to targeted marketing. Through our action plan, users can therefore choose how much of their data is being used and for what purpose, thus addressing the KVP by giving them the free will to decide how their data is being used.

How will this address the purpose?

By ensuring that biometric confirmation is needed for the usage of user data, users can feel more at ease that their data is not being mishandled and trust online payment systems more without these doubts, which makes users more likely to be willing to entrust their data to these companies, making the companies better able to serve their customers, in other words, a win-win scenario. Biometric confirmation is also much simpler and convenient compared to logging into a website or using a traditional password to confirm their use of data through buttons, which might confuse and deter the older generation who might not be the most familiar with technology, reducing the outreach and mass of audience that this system can reach out and help.

What obstacles might be encountered?

Some of the difficulties would be an unclear timeline on how long these biometrics systems can be developed and it requires large and flowing funds to keep it going that might be difficult to keep up with. Companies also might not want to comply with the system and users may find it difficult at first to use biometrics confirmation. There may also be issues during its implementation due to unfamiliarity since it will be a fairly new system when implemented.

How would we solve these obstacles?

There has been a trial period added to source out problems before the final implementation. As users may have difficulties adapting to the technology, there is also an option to split up the implementation of the technologies to help users get used to the biotech before gaze control is implemented, when it is readily available. We also aim to lobby the government for funding to ensure that sufficient funding is obtained for the project, such that there would not be a lack of funding halfway through the research process.

Bibliography

Cite the resources you consulted using the APA format.

List of citations:

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, July 27). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved August 19, 2020, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

The Biggest Email Marketing Challenges of 2018. (2020, April 21). Retrieved August 19, 2020, from https://www.litmus.com/blog/the-biggest-email-marketing-challenges/

Team, E. (2019, September 09). Big Data in the Financial Services Industry - From data to insights. Retrieved August 19, 2020, from https://www.finextra.com/blogposting/17847/big-data-in-the-financial-services-industry---from-data-to-insights

Sweeney, E. (2018, May 14). 71% of consumers worry about brands' handling of personal data, study finds. Retrieved August 09, 2020, from https://www.marketingdive.com/news/71-of-consumers-worry-about-brands-handling-of-personal-data-study-finds/523417/

Adetokunbo, C. (2002, October 31). Ubiquity: The future of internet security. Retrieved August 10, 2020, from https://ubiquity.acm.org/article.cfm?id=763941

Madden, M., & Rainie, L. (2019, December 31). Americans' Views About Data Collection and Security. Retrieved August 10, 2020, from https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/

NortonOnline. (n.d.). What are cookies? Retrieved August 11, 2020, from https://us.norton.com/internetsecurity-privacy-what-are-cookies.html

Marria, V. (2018, December 21) What a cashless society could mean for the future. Retrieved from https://www.forbes.com/sites/vishalmarria/2018/12/21/what-a-cashless-society-could-mean-for-the-future/#e037e7832638

Kohli, T. (2019, September 17). AI's contribution to the global economy will bypass that of China and India by 2030, to reach $15.7 trillion. Retrieved 13 April, 2020, from https://www.weforum.org/agenda/2019/09/artificial-intelligence-meets-biotechnology/

Collison, P. (2018, June 29). Hundreds of cash machines close as UK turns to contactless payments. Retrieved 12 April, 2020, from https://www.theguardian.com/money/2018/jun/29/hundreds-of-cash-machines-close-as-uk-turns-to-contactless-payments

Story by Yuval Noah Harari. (2018, September 13). Why Technology Favors Tyranny. Retrieved 13 April, 2020, from https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330

A Complete Guide to Big Data in Banking. (2019, November 22). Retrieved from https://us.hitachi-solutions.com/blog/big-data-banking/

What Is Big Data Analytics On Social Media? (2018, January 31). Retrieved from https://locowise.com/blog/what-is-big-data-analytics-on-social-media

How PayPal Leverages Big Data Analytics? (2017, November 17). Retrieved April 6, 2020, from https://intellipaat.com/blog/paypal-leverages-big-data-analytics/

Harari, Y. N. (2016, August 26). Yuval Noah Harari on big data, Google and the end of free will. Retrieved from https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c

What is BIG DATA? Introduction, Types, Characteristics & Example. (n.d.). Retrieved from https://www.guru99.com/what-is-big-data.html

Big Data: Meaning of Big Data by Lexico. (n.d.). Retrieved from https://www.lexico.com/definition/big_data

Rouse, M. (2019, October 25). What is Big Data and Why is it Important? Retrieved from https://searchdatamanagement.techtarget.com/definition/big-data

The 6 Challenges of Big Data Integration. (n.d.). Retrieved from https://www.flydata.com/the-6-challenges-of-big-data-integration/

5 Ways Big Data Can Benefit the Travel Industry (2020, February 7). Retrieved April 12,2020 from https://www.revfine.com/big-data-travel-industry/