Group ID: 10-14

Future Trends Report

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

Community / Organisation Studied: Future Trends

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: **Personal Information not Safe and Private**

We have crafted a survey to identify the most concerning problems with ecommerce. In the survey, we asked if the respondents trusted ecommerce, and why they trusted or did not trust ecommerce. We found that among the people who do not trust ecommerce, some people stated that they did not know how their personal information, such as credit card information or address, might be used by the ecommerce platform. We provided respondents with 7 potential problems of ecommerce and tasked them to rank the problems from the most concerning to the least concerning problem. Among the 7 problems provided, the option "personal information not safe and private" was one of them. 52.8% of respondents indicated that this was the most concerning problem to them. Consumers of ecommerce often do not have control over their personal information, once it has been given to ecommerce platforms. According to Independent.uk.co (https://www.independent.co.uk/life-style/gadgets-and-tech/news/tinder-personal-information-data-dating-privacy-how-to-see-what-app-a7968236.html), A French journalist discovered that Tinder, the dating app, had 800 pages of personal data about her. Judith Duportail claimed she discovered that the app had gathered a ton of data about her age, gender, interests, the people she had dated or spoken to, where she went and where she lived. Such personal information may be shared with 3rd parties. For example, your location would be shared with the delivery company for delivery. There isn't currently a way consumers can demand and cause the destruction or deletion of their personal information, making their information constantly vulnerable to data breaches. According to infoworld

(https://www.infoworld.com/article/3235385/is-your-data-safe-and-secure.html), significant data breaches have also been reported by Yahoo, Twitter, Target, LinkedIn, and Sony, among others.
When your information is being shared among multiple platforms, the chances of the personal information getting stolen by hackers would be inevitably higher.

Challenge 2: **Online scams**
From our survey, we found that 31.9% of survey respondents felt that "online scams" was the second most concerning problem with E-commerce. Online scams on E-commerce can include non-delivery of item after payment, items that are not authentic as claimed, or the item sold had been used before despite claims that it is new. Online scams are hard to identify because the scammers are sly and cunning. They prevent customers from viewing their reviews and their ratings so that unsuspecting customers buy their products and get scammed. This makes it hard to find and report scammers. According to The Straits Times
(https://www.straitstimes.com/singapore/courts-crime/scam-victims-lost-413-million-in-first-quarter-of-2020-e-commerce-and-loan), online scammers got away with 41.3 million dollars in total between January and March this year alone. The total amount has risen by 27.9% compared with the figure in the same period last year, showing the rising numbers in online scams.
According to https://www.businessinsider.com/online-scams, many online scammers take advantage of customers' naïveté and ignorance to trick them. Many feel that they are confident enough to spot an online scam. In the end, the online scammers are way more sly and cunning than they thought and they fall easily to online scams.

Challenge 3**: Product Ambiguity, leading to Confusion, products may not meet expectations**

In the open ended question of our survey, where we asked why respondents trusted or did not trust ecommerce, we found that among the people who did not trust ecommerce, some stated that the products sold online were rather ambiguous, and they were uncertain if they would get what is displayed online. We also learnt that a cardinal worry of most consumers is product ambiguity. In fact, product ambiguity was one of the top 3 reasons for consumers' distrust and disuse of E-commerce, with more than 25% of users stating so. Ambiguity is defined as the quality of being open to more than one interpretation; to be vague and obscure. In E-commerce, products are ambiguous as the consumer has no way of seeing the actual product. The product delivered may not be of the same quality as the one advertised, and may even be a different product altogether. This causes the consumer to become sceptical and wary of purchases from E-commerce platforms. Furthermore, since pictures and descriptions of the product are provided by the seller, they may be inaccurate and exaggerated to tempt you into buying their product.'The Daily Universe' (Online shopping doesn't always meet expectations - The Daily Universe) shows some examples of products that did not meet the buyer's expectations. It sheds some light on how students and teenagers might be affected the most by this, as they use E-commerce more frequently, especially in this COVID period. 'My Advo' (5 Most Common Problems faced by Consumers while Shopping Online) even calls E-commerce websites aggregators, which allows dubious sellers to sell faux and sub-par items without any repercussions. Moreover, websites very often do not conduct quality checks, allowing these sellers to go undetected.

Challenge 4: **Logistics-related problems**

In the survey, we asked the respondents what were some problems that consumers of ecommerce may face. Some respondents stated that there might be long delivery times, and also damaged goods, which are a form of logistics related issues. From our survey, we also found that 23.6% of respondents indicated that "Logistics-related problems" was the 4th most concerning problem. Logistics-related problems refers to slow product delivery times, or the product does not arrive on time, or the product was misplaced and does not arrive at all. Products may also be damaged during the delivery process. According to MyAdvo (5 Most Common Problems faced by Consumers while Shopping Online), Products are often lost or damaged while in transit, and order tracking systems are unable to accurately locate the product. Products often do not arrive during the stipulated time and consumers have to wait longer than expected. This creates inconveniences for consumers. According to TODAY (https://www.todayonline.com/singapore/missing-parcels-and-delivery-delays-logistics-firms-face-bottlenecks-online-orders-soar), as of late, some logistics firms in Singapore have been straining under the weight of a surge in online orders during the circuit breaker, leading to protracted delivery delays and, in some cases, parcels being lost in transit. Some Irate customers and merchants told TODAY that some of the delays have lasted for up to three weeks. Others said that the logistics firms had misplaced their items and could not locate them. As the demand has spiked by 50% due to covid-19, logistic firms may not be able to catch up with the large number of orders.

This could also happen in the future, where technology advances and more and more people get used to using Ecommerce.

Challenge 5: **Ambiguous Policies**

From our survey, we found that 23.6% of our survey respondents voted "Ambiguous Policies" as the 5th most concerning problem. Exchange policies, return policies, consumer protection policies, seller protection policies, etc may be vague and not clear. This may lead to confusion and misunderstandings which can cause a lot of inconvenience. According to MyAdvo (5 Most Common Problems faced by Consumers while Shopping Online), some shopping websites have no website policies and others have unclear and confusing policies. The vague policies would make consumers confused about refund and return of products and product description problems in e-commerce. With no or unclear policies, sellers can reject a consumer's claim to return the product or refund the money. Some websites are also unclear with regards to warranty on goods and consumers may end up purchasing faulty products with no warranty can the products cannot be returned. According to privacypolicies.com (https://www.privacypolicies.com/blog/terms-conditions-mistakes/), a vague term & conditions may lead to a misunderstanding by consumers, which can create problems for both the consumer and the company. Facebook faced legal issues, as they included a limitation of liability that was too broad, and caused confusion.

Group ID: 10-14

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) # 1, 2

Underlying problem:
With the advancement of technology in 2030, more people would be using eCommerce, making consumers more vulnerable to personal data breaches and scams. (condition and fsp) How might we improve the current measures of E-Commerce platforms (key verb phrase) in order to give consumers a better sense of security and trust? (purpose)

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: **Improve Security firewall**

What?

The security firewall of the ecommerce platform could be improved, in order to make it harder for hackers to steal personal information.

According to the Official website of the Department of Homeland Security (https://us-cert.cisa.gov/ncas/tips/ST04-004#:~:text=Firewalls%20provide%20protection%20against%20outside,or%20network%20via%20the%20internet), a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically prevents malicious software from accessing a software via the internet. A firewall controls traffic between networks, reducing the chances of the software getting hacked by malware or viruses.

Why?

It helps to eliminate viruses, thereby reducing the chances of hacking. The Firewall would reduce the chances of hackers implanting viruses into the software of ecommerce platforms. This would prevent them from assessing the databases of eCommerce platforms and steal information, such as credit card information or personal information. The stronger security firewall would also give consumers a better sense of security as well as trust in ecommerce platforms.

Who/Where?

It would be implemented by companies that operate E-commerce platforms.

How?

The existing firewall in the ecommerce platforms can be improved either by updating the existing software or by implementing a more advanced security firewall.

When?

As this does not require futuristic technology, the firewall can be updated and installed by 2021. However as technology gets more advanced in the future, hackers may become

more advanced and conventional firewalls may not be as effective as before. Therefore, the security firewall must become more advanced in the future as well.

Solution 2: **Implement AI into ecommerce platforms**
What?
It would be an artificial intelligence system that is incorporated into eCommerce platforms. The AI system could also be taught to detect scammers before anyone falls victim to the scam. Some scams are "too good to be true". Goods sold at a much cheaper price than usual could be suspicious. The AI could compare the goods sold to the average price of the goods. If the price that the item is sold at is much cheaper than the normal average price one would find, and there are no sales going on, it would prompt the personnel in charge to investigate. This will be flagged up for the seller to produce product authenticity cert/barcode. If Sellers are unable to produce a product authenticity cert, then they cannot use the word authentic and the actual brand name in their product. The system could also have access to data from past cyber incidents, which it could analyse to identify potential threats to the security. It can also analyse the existing security measures put in place to find any security holes, and prompt the personnel in charge to make amendments to the system.

Why?
The system would narrow down the potential scammers on the ecommerce platforms, and is more efficient as the personnel in charge would not have time to look through the large number of sellers. This would help in removing scammers from eCommerce platforms. It can also narrow down the potential threats to the security or the potential problems in the security system, making it easier for the people in charge to address the problems as soon as possible. This would also give the consumers of eCommerce a better sense of security, as the security would be stronger.

According to ZDNet (https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/), Artificial Intelligence (AI) and Machine Learning (ML) will be an important tool in combating potential cyber threats. Millions of cyber incidents can be carefully analysed , and common scams and accounts can be easily detected and banned.

Who/Where?
Companies that operate Ecommerce platforms will implement this system for better security.

How?

The AI system can be downloaded into the operating system of the Ecommerce platform.

When?
Here is our proposed timeline: In 2020, we would propose the idea to a tech company, and gain approval for the start of our project. By 2025, the first version of the system should be completed, and trials can begin. Between 2025 and 2028 would be the testing period. Constant adjustments and improvements need to be made to the system, and feedback can be collected from trial clients. By 2028, the system can be rolled out and tested by trial clients. Adjustments and updates can also be made based on the performance of the system. In 2030, the system can be rolled out to ecommerce industries for commercial use.

Solution 3: **Regular software updates and security checks**
What?
Regular software updates will update the websites, patching up potential loopholes and vulnerabilities. Updates will also strengthen cyber-security by improving the software's stability, and removing outdated software that might be exploited by hackers. Security checks, when done frequently, can detect malware and viruses that might be present in the software. These viruses can be isolated and removed quickly.

Why?
Without constant updates and security checks, the software can become outdated and obsolete very quickly. New types of malware and viruses will easily be able to compromise a website if the software is not up to date. Malware may go undetected if regular security checks are not conducted, causing data and personal information to be stolen. The improvement in security would also make consumers feel more safe and secure while using the ecommerce platforms, which also allows them to have more trust in the ecommerce platform.

According to McAfee (https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important), the Equifax data breach potentially affected 143 million Americans, with Social Security numbers, birth dates, and home addresses exposed. The hackers were able to access the credit reporting agency's data through a known vulnerability in a web application. This could have been fixed with a software update since 2 months before the data breach, but the company failed to update the software. This reveals that software updates play an important role in the security of the ecommerce platforms.

Who/Where?
It can be implemented by various ecommerce companies.

How?
The frequency of software updates and security checks can be increased.

When?

This could be done by the year 2021, as no futuristic technology would be needed.

Solution 4: **Delete personal data after use**
What/Who/Where/How?
The government could implement policies to force ecommerce industries to delete the user's data off their data banks after the transactions.

Why?
With this recommendation, it reduces the chances of hackers stealing personal information since there would not be any personal information to steal.This would also give consumers a better sense of privacy and security. Eventually, companies would start gaining the trust of consumers when they stop making the most of consumers' data and start getting rid of their data entirely.

According to security.org (https://www.security.org/resources/consumer-data-security/), Until 2003, receipts contained both the full credit card number and the expiration date. That year, the Federal Trade Commission ordered a change in the rules. Businesses were not allowed to display more than the last five digits of a credit card, and they cannot show any part of the expiration date. However 15 years later, it was still not enough to leave private information off the paper receipts due to the advancement of hackers and scammers. Information had to be deleted after the transaction was completed. According to the huffpost (https://www.huffpost.com/entry/6-ways-to-protect-customer-data_b_59cd51f9e4b04575111f3963?guccounter=1), they also suggested getting rid of personal information after use. They also claimed that it would reinforce the consumers' trust in the ecommerce platform.

When?
The policies can be implemented as soon as possible as there is no futuristic technology involved. It could be fully enforced in the year 2022 for ecommerce companies to accept and adjust to the policies.

Solution 5: **Consumer education**
What/Who/Where?
Lesson packages could be made to educate consumers about their rights, what happens to their personal data, how they can take legal action if they are scammed, return policies, etc. It would include simplified terms and conditions, and cover most important details such as return policies. It could also educate consumers on how to detect scammers, and buy from reputable sellers with positive seller ratings.

Why?
The main purpose of the lesson packages would be to assure consumers that they are safe on the ecommerce platforms, in order to give them a better sense of security and trust. They can also make better decisions online such as buying from reputable sellers to reduce the chances of being scammed.

According to CMS Wire, (https://www.cmswire.com/content-marketing/the-importance-of-consumer-education-in-todays-data-driven-purchasing-journey/), "The more information a buyer has, the better able they are to make a good choice for themselves," explained Alice Stevens, senior content strategist at BestCompany.com. The article also stated, "Consumer education is crucial for brands because it can impact every aspect of the customer journey. A strong consumer education strategy can lead to thought leadership, better understanding of what your brand offers and improved conversions in the long run." This shows that consumer education would allow consumers to have a better trust in ecommerce.

How/Where?
The lesson packages can be incorporated into the ecommerce platforms, for example via their terms and conditions page or their faq page.

When?
The lesson packages could be made by the year 2021, and ecommerce companies can be encouraged to incorporate these lesson packages within the same year.

Group ID: 10-14

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: Feasibility

Criterion 2: Effectiveness

Criterion 3: Resource Efficiency

Criterion 4: Most Positive Impact

Criterion 5: Sustainability

Group ID: 10-14

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.

	Criteria One: Feasibility Points: 5 (Weightage: 2)	Criteria Two: Effectiveness Points: 5 (Weightage: 5)	Criteria Three: Resource Efficiency Points: 5 (Weightage: 1)	Criteria Four: Most Positive Impact Points: 5 (Weightage: 4)	Criteria Five: Sustainability Points: 5 (Weightage: 3)	Total:
Solution 1: Improvement of Security Firewall	5	3	5	4	4	58
Solution 2: Implementation of Artificial Intelligence	3	5	4	3	4	59
Solution 3: Software Updates & Security Checks	5	3	4	4	4	57

Solution 4: Delete personal data after use	4	3	5	3	3	49
Solution 5: Consumer Education	5	2	5	3	4	49

Step 5. Develop an Action Plan and Evaluate its Feasibility

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 2):
It would be an artificial intelligence system that is incorporated into eCommerce platforms. The AI system could also be taught to detect scammers before anyone falls victim to the scam. Some scams are “too good to be true”. Goods sold at a much cheaper price than usual could be suspicious. The AI could compare the goods sold to the average price of the goods. If the price that the item is sold at is much cheaper than the normal average price one would find, and there are no sales going on, it would prompt the personnel in charge to investigate. This will be flagged up for the seller to produce product authenticity cert/barcode. If Sellers are unable to produce a product authenticity cert, then they cannot use the word authentic and the actual brand name in their product. The system could also have access to data from past cyber incidents, which it could analyse to identify potential threats to the security. It can also analyse the existing security measures put in place to find any security holes, and prompt the personnel in charge to make amendments to the system.

Why should it be implemented? The system would narrow down the potential scammers on the ecommerce platforms, and is more efficient as the personnel in charge would not have time to look through the large number of sellers. This would help in removing scammers from eCommerce platforms. It can also narrow down the potential threats to the security or the potential problems in the security system, making it easier for the people in charge to address the problems as soon as possible. This would also give the consumers of eCommerce a better sense of security, as the security would be stronger.

Companies that operate Ecommerce platforms will implement this system for better security. The AI system can be downloaded into the operating system of the Ecommerce platform.

Here is our proposed timeline: In 2020, we would propose the idea to a tech company, and gain approval for the start of our project. By 2025, the first version of the system should be completed, and trials can begin. Between 2025 and 2028 would be the testing period. Constant adjustments and improvements need to be made to the system, and feedback can be collected from trial clients. By 2028, the system can be rolled out and tested by trial clients. Adjustments and updates can also be made based on the performance of the system. In 2030, the system can be rolled out to ecommerce industries for commercial use.

While the AI system has its positives, it may also come with some problems of its own. As the AI system uses advanced technology, it may be costly to implement. The AI system would require extensive testing to ensure that it is good enough to improve the security of eCommerce platforms, which may need a lot of time before it can be implemented. There may also be an over reliance on the AI system to identify problems in the security. This could have adverse consequences if the AI were to stop working or get hacked.

We have crafted a survey to get feedback about the feasibility and effectiveness of our action plan. 72% of our respondents believe that our proposed solution would be effective at solving the problem. 76% of our respondents agree that the solution is feasible if implemented in the year 2030. However, some respondents stated that the AI system may not be secure and stable enough to ensure the security of ecommerce platforms. They also do not really trust Artificial Intelligence as it might be hacked or malfunction. It could also be costly and time consuming to implement.

Artificial Intelligence already exists in the present time. With the advancement of technology in the future, we believe that there would be many more applications for artificial intelligence and it would be possible for AI to be implemented into eCommerce as well. However it might take time for companies to accept this system into their eCommerce platforms as such a system would be alien to them.

Bibliography

List of References: Top 5 security threats facing eCommerce today. (2020). Retrieved 10 August 2020, from https://www.loop54.com/blog/top-5-security-threats-facing-e-commerce-today
http://systemarchitect.mit.edu/docs/fang19a.pdf
WONG, C. (2020). Scam victims lost $41.3 million in Q1; e-commerce and loan scams among most common. Retrieved 11 August 2020, from https://www.straitstimes.com/singapore/courts-crime/scam-victims-lost-413-million-in-first-quarter-of-2020-e-commerce-and-loan
Protecting Customers - Security.org. (2020). Retrieved 11 August 2020, from https://www.security.org/resources/consumer-data-security/
Palmer, D. (2020). AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know | ZDNet. Retrieved 11 August 2020, from https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/
Davis, G. (2020). Why Software Updates Are So Important | McAfee Blogs. Retrieved 11 August 2020, from https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important/
BeCyberSafe.com | How To Spot A Scam. (2020). Retrieved 11 August 2020, from https://www.becybersafe.com/online/avoiding-scams.html
Top 5 security threats facing eCommerce today. (2020). Retrieved 18 August 2020, from https://www.loop54.com/blog/top-5-security-threats-facing-e-commerce-today
Awan, A. (2020). Is your data safe and secure?. Retrieved 18 August 2020, from https://www.infoworld.com/article/3235385/is-your-data-safe-and-secure.html
Tinder has a terrifying amount of data on you. Here's how to see it all. (2020). Retrieved 18 August 2020, from https://www.independent.co.uk/life-style/gadgets-and-tech/news/tinder-personal-information-data-dating-privacy-how-to-see-what-app-a7968236.html
WONG, C. (2020). Scam victims lost $41.3 million in Q1; e-commerce and loan scams among most common. Retrieved 18 August 2020, from https://www.straitstimes.com/singapore/courts-crime/scam-victims-lost-413-million-in-first-quarter-of-2020-e-commerce-and-loan
The 11 most sophisticated online scams right now that the average person falls for. (2020). Retrieved 18 August 2020, from https://www.businessinsider.com/online-scams-internet-phishing-2019-3
(2020). Retrieved 18 August 2020, from http://systemarchitect.mit.edu/docs/fang19a.pdf

LIMITED, M. (2020). 5 Most Common Problems faced by Consumers while Shopping Online. Retrieved 18 August 2020, from https://www.myadvo.in/blog/5-most-common-problems-faced-by-consumers-while-shopping-online/

Missing parcels and delivery delays: Logistics firms face bottlenecks as online orders soar. (2020). Retrieved 18 August 2020, from https://www.todayonline.com/singapore/missing-parcels-and-delivery-delays-logistics-firms-face-bottlenecks-online-orders-soar

Agreement, 7. (2020). 7 Mistakes You're Making With Your Terms and Conditions Agreement - Privacy Policies. Retrieved 18 August 2020, from https://www.privacypolicies.com/blog/terms-conditions-mistakes/

Understanding Firewalls for Home and Small Office Use | CISA. (2020). Retrieved 20 August 2020, from https://us-cert.cisa.gov/ncas/tips/ST04-004#:~:text=Firewalls%20provide%20protection%20against%20outside,or%20network%20via%20the%20internet.