1 The Emotional App

You are designing and are about to launch a mobile-only social media app which will seek to understand the emotional condition of the user, using multiple inputs such as motion sensing, facial expression recognition, voice stress measurement, user interactions with the app's content, and the sentimental analysis of user-inputted text.

Its declared purpose is to enable services to interact more empathetically with users and serve more relevant content. You propose to monetize it by serving ads at times when the user is more likely to buy.

A core team member with a Cambridge CS education that has previously studied the ELE course claims that this monetization technique is predatory as it will be exploiting users at times of emotional vulnerability.

As the capitalistic enterprising mastermind behind the genius app idea, you were initially included to fire this colleague as their point-of-view would result in less ad revenue. However, your investors have also raised a concern that this app will be able to diagnose depression, and that in consequence, you may be storing substantial amounts of sensitive personal information.

Discuss this problem from the viewpoints of both data protection law and ethics.

1.1 Draft

- Introduction

  A brief discussion of how outdated laws will allow an ethically questionable app to be released.

- GDPR 1

  Discuss the provisions of the GDPR.

- GDPR 2

  Discuss the rights of the GDPR.

- Other legal concerns

  Discuss compliance with RIPA and the associated ethics.

- Extremism and racism

  Discuss other potential legal issues – promoting political hate material and racism for money. Exposing vulnerable people to this material will promote division.

- Exploitation

  We will learn more about the emotional state of users of the app. This will be correlated with peoples financial situation. Thus we can serve more tailored adverts. This could lead to dangerous adverts such as scams being served "I made $113948 in 3 weeks – see how!". Or serving "energy-saving tips" involving placing tealights under flowerpots which the metropolitan police has told people not to do due to risk of fire to people who are cold during energy crises.

- Facebook Trial

  Discuss Facebooks trial which found users responded more to negative content. Since we know more about peoples emotional state, we will know more about what they view as negative. We will therefore *always* provide people with material slightly more negative than how they are currently feeling. Think providing depressed people with material promoting self-harm and suicide. IE Molly's Law.

- Professional standards of ethics

  Discuss the professional standards of ethics: ACM or approval from ethical committees.

- Conclusion

  A brief overview of all the topics covered and reiteration of the most important points.

1.2 The Essay

It is well-known that laws surrounding technology are consistently a decade behind reality. As a result of this, there are often cases where what is legal is not ethically correct. The proposed app and its monetization strategy is an example of this. Although the app can be made to comply with the GDPR, it would remain grossly unethical; cause great harm to its users and likely promote racism and political divisions. While there are proposals such as "Molly's Law" which would give social media platforms a duty-of-care to their users and would make the apps current model illegal; the app and its monetization strategy would currently be legal.

The GDPR is EU regulation designed to give data subjects ownership of their own data; limiting the amount of data that companies can collect, forcing them to collect data only by legitimate routes and obligating companies only to use data for the purpose the user consented. The GDPR does not regulate the ethics of how data is used – only force the company to make the user aware of how it is used. The GDPR has a number of provisions and rights. The six provisions of the GDPR are: data must be collected fairly and lawfully; data may only be used for the original purpose; data must be adequate, relevant and not excessive; data must be accurate and kept up-to-date; identifiable data must not be kept for excessive periods of time; and data must be processed securely and protected against loss or damage. The app can be designed in such a way to comply with all of these.

The GDPR also gives "data subjects" a number of rights, three of these are especially relevant to the app. The right of access gives all data subjects the right to see all data which is held on them; the app manufacturers will have to is designed the app such that this data can be collected or face significant legal repercussions and a costly fee to rebuild the app. The right to erasure permits users to request a total deletion of all the data the company holds on them. The app must be able to do this; they must design the app such that users can delete their accounts and all associated data. The right to object allows users to object to the use of their data in a particular way. This right is absolute when the use is marketing. In order to comply, the app will have to provide the ability for users to disable personalised adverts.

In 2016, the law was changed to legalise the interception and surveillance that security agencies such as GCHQ were performing. The Act implemented is called IPA (Investigatory Powers Act). The provision most relevant to the app (inherited from RIPA [Regulation of Investigatory Powers Act]) states that companies may be required to supply information to government bodies (in an intelligible form) and not inform their clients that they are doing so. If the app were to become popular, it's likely there would be IPA requests. The app should create frameworks to enable the collection of this data quickly.

The affect of social media on politics has gone under global spotlight and scrutiny over the last decade. To maximise engagement, users are recommended content which they are most likely to click on – content which reinforces their own beliefs. This creates cliques or cults such as QAnon where members continually reinforce each others beliefs and continue to promote hate, racism and extremism. The people who are most susceptible to being inducted into extremist groups are the most vulnerable – those who are suffering from depression or are social outcasts. Our social media platform is likely to pick up on this and recommend content which they are more likely to interact with – extremist content. Extremist adverts or those which promote hate are most likely to be shown to the most vulnerable members of society. Our app would be monetizing the spread of extremism, hate and political division.

This is highly unethical and likely to cause a backlash which would affect revenue and public image of the company.

Many adverts are misleading or even scams. They peddle fake information in an attempt to make a mundane or useless product or service "clickbait" enough to "beat" recommendation algorithms. These adverts are designed to relate to and pray on a very specific audience. With additional information about peoples mental state, the app will be able to tailor these manipulative adverts to those most likely to fall for them. For example, early in December 2022 dangerous online advertisements almost caused a second Grenfell. A tower block was evacuated after a resident suffering from the cold tried an "energy-saving trick" which had been advertised to them online. The police and Fire Brigades begged the public not to use this due to the high risk of fire. As of late December 2022 this advert was still being run by Google and targeted at that same demographic – as they are the most likely to engage with it. An app which has additional information about the users emotional state will be able to supply these manipulative and dangerous adverts to those most likely to fall for them at exactly the wrong times. Our app would therefore be profiting from dangerous scams and fire call-outs.

Attempting to maximise engagement with additional knowledge about a users mental state will result in exposing users to negative emotions and propagating depression and self-harm. In 2014, Facebook launched an experiment on 700000 users to see what type of content users engaged with the most. This experiment was not consented to by users and is widely regarded as one of the most unethical experiments in modern history. The researchers found that users engaged most with negative content. Knowing more about a users mental state will enable the app to provide the most engaging stories to them – the negative content with which they are most likely to engage. This will spread negative emotions: hate and depression. If we know that users are already depressed, then negative content relative to them will promote self-harm and suicide. Recommending content such as this disregards any duty-of-care and is known to have caused suicides. Therefore the app will survive only by damaging its users mental states and in the worst case promoting self-harm and suicide. Many advertisers may be unwilling to sponsor this: "this post promoting self-harm is brought to you by …".

Modern software development is not covered ethically by the law – there are many legal actions which are totally unethical. In order to counteract this, ethics boards have been set up which look at plans ethically. Approval from one of these boards could cement the app as ethical – and if not, could help transition it into one which would be. Professional ethical guidelines also help bridge the gap between ethical and legal in the technology industry. ACMs guidelines state that computing professionals should contribute to society and human well-being. This app is likely to contribute to human misery (by worsening depressive disorders and spreading extremism); therefore is unethical by professional ethical standards.

Compliance with data protection laws is not problematic – the app must ensure users are aware of the collection of data and provide provision to extract data from the system. However, there are many other legal issues surrounding the app. Due to outdated laws, the app would be legal in the UK. However, recent attempts to give social media companies a duty-of-care would make the app illegal. The app is grossly unethical. It's likely that the app would exploit vulnerable users, spread hate and eventually alienate itself from investors over ethical concerns.

2 2019 Paper 7 Question 3

https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2019p7q3.pdf

(a) What do sections 1, 2 and 3 of the Computer Misuse Act 1990 prohibit?

Section 1. Unauthorised access to computer material.

This prohibits seeing data you are not allowed to see – finding backdoors or hacking to gain access to data you are not meant to see.

Section 2. Unauthorised access to computer material with intent to commit or facilitate further offenses.

This is a separate offense to allow for the more serious crime of accessing data and intending to use it for something to have a higher maximum sentence.

Section 3. Impairing the operation of a computer.

The way in which the computer has been impaired is broad.

This covers unauthorised modification of data – the reliability of the data has changed and so the computer no longer operates in the intended way.

This also covers denial-of-service attacks where a computer is no longer able to operate due to the high load.

There are later subsections of part 3 which prohibit creating, making or supplying articles intended to be used to break the Computer Misuse Act.

In all sections of the CMA, the attacker must know that they are not authorised to access the data; the attack does not have to be against any specific computer or program or data. This means a large company which was attacked does not have to find the particular bytes and the particular computers which were attacked.

(b) Eve is operating a DDoS-for-hire service and has recruited 100,000 CCTV cameras into a botnet. If Mallory pays Eve $2 to take down a gaming teamspeak server for five minutes, what offences, if any, are being committed by Eve and Mallory?

Section 3 of the computer misuse act prohibits "performing any act intended to impair the operation of a computer". Mallory has performed such an act: paying Eve to DDoS the gaming teamspeak.

Eve can also be persecuted under section 3 of the computer misuse act – Eve is controlling the botnet; so has made acts to impair the operation of a computer. Namely the servers running the gaming teamspeak.

As of 2007, the Computer Misuse Act also prohibits creating, obtaining or supplying artefacts used to break the Computer Misuse Act. Eve has supplied an artefact (a DDoS-for-hire service) which is used to break the Computer Misuse Act. Depending on the exact semantics, Eve has also either created or obtained the artefact; depending on whether Eve wrote the code that built the botnet.

(c) How might the Wimbledon case (R v. Lennon 2005) apply to this case?

In the Wimbledon case, a 16-year old teenager (David Lennon) worked for a company for three months until he was fired. A year later, he decided to DoS them using the program Avalanche. This sent 5 million emails to the company over a weekend and took down their email server and caused an estimated £18000 damage.

Since Lennon was initially a minor when he committed the act, the course was dealt with in the Youth Court. The defence argued that there was "no case to answer". The persecution attempted to argue that sending so many email modified the internal state of the email server and was therefore an unauthorised modification under the CMA section 3. The defense countered that a single email would do the same – since the purpose of the email server was to receive emails this was authorised. The defense then argued by induction that there could be no threshold above which any amount of emails would be unauthorised. The youth court agreed with the defense and dropped the case.

This was taken up in a court of appeals a year later. The DPP ruled that the consent should be similar to "if you asked beforehand if you could send 5m emails, would you be allowed to". Since Lennon had used the program Avalanche, and the company had never consented to receiving unsolicited emails from DoS software, none of the emails

were consented and therefore even sending the first email from the Avalanche software was in breach of the CMA section 3.

Lennon was then sentenced to 3 months of house arrest, where he was tagged. This ended shortly before he started university.

This landmark ruling states that there is no threshold beyond which the CMA was breached; any Denial of Service attack at all is a breach of the CMA. Therefore the "the site was down only for five minutes" is no defense against the law!

3 2017 Paper 4 Question 7

https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2017p4q7.pdf

You are commissioned by a customer to design a toy robot that children will be able to control using a smartphone app. This app will also enable them to program the robot using a simple scripting language. To simplify the networking, all communications between the app and the robot will flow over wifi via your server.

(a) Discuss the legal and ethical implications

Since the target audience of this toy is children, the company will be unable to form a contract with them (UK law forbids making contracts with children under the age of 13). Therefore the company will be unable to disclaim liability and would be responsible for any injury caused by the toy. Instead, there is separate legislation which the toy must conform to: the Toy Safety Regulation. This regulation sets out a number of safety criteria which toys must comply with to be sold in the UK. These are broadly commonsense and intuitive – if the company takes reasonable measures and places warnings for any obvious risks (ie battery cover as a choking hazard) then the robot can pass the Toy Safety Regulation.

The toy could be used for or cause harm in other ways. Consider the extreme example of commands to the toy being used to detonate a bomb. The command to detonate the bomb was sent through the company's servers. The company (and the ISP) would be able to apply the "mere conduit" defence and would not be responsible for the detonation.

The company may want default ownership of code written in its app for use in tutorials or marketing similar. By default, copyright is owned by the original producer of the material; and moral rights are permanently owned by the original producer. However, since children cannot make contracts, they cannot agree to terms and conditions which give ownership of their code over to the company. Ethically, the children have ownership of their own code; the company may wish ask for permission to use their code or even purchase their code.

Although there is no legal obligation to do so, the company should attempt to provide encrypted transmission between the Toy and their servers. Users can put arbitrary code and inputs into the app; it's possible they may input sensitive information. The company morally has a duty-of-care to the children using it's app – it would be unethical not to protect the information they are sending. The company should therefore encrypt messages sent between the server and the Toy. The easiest way to do this would be using TLS.

E-waste is a growing problem: the lifetime if electronics is short and they contain many toxic chemicals. Eventually, the children will grow out of the Toy Robot and throw it away where it will end up either in landfill or the ocean. The company should endeavour to make the robot as environmentally-friendly as possible by using few toxic materials.

(b) Your customer decides to incorporate a microphone so that the robot can also recognise spoken commands. To save battery life, the speech recognition will be done in the server. What effect does this have on the ethical and legal situation.

Potentially personal audio data is now flowing through the company servers. Legally, the company must process this in compliance with the GDPR.

- Data must be collected fairly and lawfully
- Data must be used only for the intended purpose
- Data must be adequate, relevant and not excessive
- Personally identifiable information must not be kept for excessive periods of time
- Data must be kept accurate and up-to-date
- Data must be processed securely and protected against loss or damage.

Many of the app's users will be under 13 and must acquire parental consent to use the app – young children are unable to form contracts and therefore cannot agree to their voice data being processed.

Since the company is now no longer a "mere conduit", they are more likely to be liable for damages caused by the robot: if the robot mis-hears a command then the company is liable for the damage caused. This can be alleviated with stronger warnings and a further requirement for parents to consent that the robot's voice recognition may not be perfect.

Unfiltered information is now flowing into the company's servers. This could also contain sensitive information which the robot was not meant to overhear such as bank information or passwords. Storing records of all audio the robot hears is excessive (in breach of the GDPR) and would contain enough sensitive information to make the company a target for criminal organisations who could run voice recognition AI searching for keywords relating to banking or passwords. The company is required to protect the data they collect; so communications would need to be well-encrypted (perhaps using TLS). Collecting and storing thousands of hours of speech data from thousands of households around the country is morally unjustifiable! The company should therefore not store speech data or transcripts.

The company has a microphone in thousands of households; this may be of interest to GCHQ who can force the company to disclose information under the IPA.

(c) What practical advice can you give your customer about mitigating the legal risks?

The company should have warnings, usage guidance and terms of service which require parental consent. Furthermore, the company should appoint a data protection officer to ensure full compliance with the GDPR (and take the blame if something does go wrong). The company should also be clear that any legal issues are to be resolved in a UK court and put firm caps on the legal costs associated with any disputes to minimise risk. The company should be transparent about the processing done to ensure any risks are exposed early before they become scandals. Communication should all be encrypted to avoid wiretappers finding personal information.

(d) Your customer now wants to include a camera so that the robot can recognise gestures as well. Does this create any further ethical or legal risks, and if so, what might be done about them?

The company must not store any images. The robot is intended to be used by children and as such may be stored in their bedrooms. It is likely that over extended periods of use, it would see indecent images of many of it's users (children) changing. It is not legal to possess indecent images of children and so the company must not store any images. Furthermore, it must take even greater care to encrypt data. I would suggest passing all images through an encoder (trained to minimise error of gesture recognition with specific effort taken to ensure that accurate reconstruction of the original image is not possible) and only send this encoded data from the toy. This would also alleviate ethical issues and issues regarding compliance with the IPA –

the company does not have video feeds of users houses and so cannot send them to GCHQ. It would be strongly advisable to take extreme precautions to guarantee no child pornography/child exploitation lawsuits: the worst possible publicity for a Toy manufacturer. Further consent for recordings is required in all cases.

By using gestures, the company opens itself up to racial bias lawsuits: many companies which use facial recognition or gestures have faced lawsuits about racial bias for systems which do not work properly for people with non-white skin. For example, Uber was sued in 2021 over bias facial recognition software which was unable to recognise black drivers and terminated several black drivers accounts. The company should therefore take care to ensure that the gestures are trained on people with all colours of skin.

If the company were to work only on encoded data, the vast majority of ethical concerns would be removed: the gestures themselves are not sensitive information. Many users would rightfully question the point of sending this data to be processed on a server given that the Toy would already have to run an encoder – the majority of the work for gesture recognition.

If the images were not encoded, users would have significant ethical issues regarding surveillance: the Toy would become a live camera in thousands of houses. This could leak intimate images and ruin peoples lives.

(e) How might the situation be affected by Brexit?

The GDPR is an EU regulation. Post-brexit the UK may introduce new legislation which supercedes the GDPR. This could mean some of the precautions necessary when processing speech data may not be required. In reality, any company which processes EU citizens data must comply with the GDPR. If the manufacturers want to sell the Toy in Europe (which is rational) then they will have to comply with the GDPR even after Brexit.

The UK is currently affected by an EU law which states that you cannot exclude liability for death or injury. On leaving the EU, the UK would be able to change this should we want to. This could allow the company to write off injuries completely and may be able to release less child-proofed toys in the future.

The age at which children can make contracts is 13 in the UK. In many other EU countries this is 16. Prior to Brexit, there was a chance that the UK age could be influenced by our partners leading to precautions necessary with under-13s being extended to under-16s. Post-Brexit, this will not be a realistic issue.

The primary concern with image data is indecent images of children. While some EU laws do pertain to child exploitation, it is unlikely that they will be loosened post-Brexit.