KNOX
GRAMMAR
SCHOOL

STATE

DA VINCI DECATHLON 2022

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS IN YEARS 9, 10 & 11

IDEATION

TEAM NUMBER _____

Total	Rank
/60	

THE CHALLENGE

FACE THE MUSIC

BACKGROUND

One of the fastest growing **technologies** in our world is that of **pattern recognition**. Pattern recognition is a form of AI (artificial intelligence) used in a plethora of fields, including data analysis, image analysis, computer graphics, machine learning, information retrieval and much more.

Pattern recognition necessarily requires the **storage** of **data**, which is then drawn upon later by the AI in order to achieve recognition. One area in which this has caused a significant degree of **controversy** is **biometrics** – the storage of information about a person's biological and physical features, ranging from speech to fingerprints to body shape. Undoubtedly, in many applications the use of pattern recognition technology in connection with biometrics is extremely **useful** and simultaneously **benign**, such as unlocking one's smartphone, but there is certainly the **potential** for much more sinister operations.

Delving into even greater specifics, the field of **facial recognition technology** is one where the boundaries of what is possible, and of what is **ethical**, are rapidly being redefined. It goes without saying that facial patterns – the vectors between our eyes and our nose, our nose and our mouth, etc – are incredibly **unique**, and also, problematically, rather **difficult to conceal**, and this means that it is becoming effortless for AI technologies to identify particular individuals, even among a crowd of faces.

The question, therefore, is this: how far should technology be allowed to go?

THE DESIGN CHALLENGE

Imagine that you are the CEO of Focus AI Ltd, a company that has recently developed the **most advanced** facial recognition technology known to the modern world. As the leader of your organisation, it is your responsibility to frame the company's **policy** for how you will allow your technology to be **licensed** to third parties: governments, companies, and other forms of organisation. This is the focus of your challenge for this paper.

First off, there are two core aspects to any policy of this kind: **ethics** and **business strategy**. Your company must, undeniably, make a **profit**, and in this scenario, the potential for profit is immense. However, you must also maintain your company's **reputation** and standing as a good **global citizen**. This means balancing profit potential against allowing the unethical use of the technology that you control.

By way of additional context, Focus AI Ltd has, in the past, provided technology to the following groups

- Governments, and in particular their militaries, law enforcement, and surveillance/spy agencies;
- Private security firms;
- Smartphone and computer companies;
- Advertising firms;
- Schools;
- Social media sites;
- Banks and other financial institutions;
- Airlines and other transport organisations;
- Cosmetics manufacturers;
- Disability charities; and
- Casinos.

Ultimately, your task is to **develop a broad policy framework**, outline the **degree** to which you are willing to push the ethical boundaries of facial recognition technology. This will, crucially, involve identifying the **main uses** that you **will** and **will not** allow, and why. This comprises your **'vision statement'.**

Additionally, that policy must include a **strategy** for how you will **convince** both the members of your company *and* your customers that your chosen policy framework is most desirable. The **'ideate'** section of this task is where you should debate such strategies.

Finally, your **'prototype'** section can represent either your vision statement (i.e. it can involve the authoring of a more detailed version of your policy), or it can depict the way in which you will implement the strategy you have chosen after the processing of ideating, **or it can include both!**

To further assist you in completing this challenge, **stimulus material** is provided within this paper, following the marking guidelines. You are encouraged to **refer** to this material in your answers where appropriate.

Finally, you are required to follow the **four-step process of ideation**, most of which has already been briefly referred to above. This is outlined below and is also set out in your answer booklet. It accords with the marking guidelines, which are provided on the following page.

EMPATHISE (Ethical Decision-Making Framework) (15 marks)

This involves evaluating what 'ought to be done', through considering rights, obligations, fairness, the benefits and detriments for societies and other virtues. Reaching a final decision involves a degree of conviction and belief in what is 'the right thing to do'.

DEFINE (Design Brief) (10 marks)

Here, you must identify the problem, outline the ethical issues, evaluate the challenges and research findings, and identify possible solutions.

IDEATE (Reflection) (25 marks)

You must then reflect on their solutions and whether they will be viable. A preferable solution should be identified, and any unanswered questions should be addressed. Issues of implementation are also crucial to reflect upon.

CREATE (Prototype) (10 marks)

Finally, a design for how your ideas and solution will be disseminated must be produced. This could be a story-board, mind-map, diagram, model, narrative or any other appropriate medium. Critically, an audience must be able to understand the process of dissemination by examining this prototype.

MARKING GUIDELINES

1. Empathise (15 marks)

QUESTIONS	LIMITED	SOUND	OUTSTANDING	TOTAL
1: Factors contributing to the issue	0-1	2-3	4	
2: Consequences if not addressed	0-1	2-3	4	
3: Identify different perspectives	0-1	2	3	
4: Identifies barriers to addressing the issue and why they are barriers	0-1	2-3	4	
			TOTAL	/15

2. Define (10 marks)

ASPECT	LIMITED	SOUND	EFFECTIVE	OUTSTANDING	TOTAL
Vision Statement: What do you want to achieve?	0-1	2-3	4	5	
Importance of Vision Statement	0-1	2-3	4	5	
				TOTAL	/10

3. Ideate (25 marks)

ASPECT	LIMITED	SOUND	OUTSTANDING	TOTAL
Possible Solution #1	0-1	2-3	4	
Possible Solution #2	0-1	2-3	4	
Possible Solution #3	0-1	2-3	4	
Choice of solution	0	1	2	
Justification of solution	0-1	2-3	4	
Implementation: when, where, who?	0-1	2	3	
Dissemination: how to succeed with the solution	0-1	2-3	4	
			TOTAL	/25

4. Create (10 marks)

ASPECT	LIMITED	SOUND	EFFECTIVE	OUTSTANDING	TOTAL
Originality and creativity	0-1	2-3	4-5	6	
Clarity and communication of ideas	0-1	2	3	4	
				TOTAL	/10

TOTAL: /60

ADDITIONAL STIMULUS

'Facial Recognition Is Everywhere. Here's What We Can Do About It.' (T Klosowski, *The New York Times – Wirecutter*, 15 July 2020)

Facial recognition—the software that maps, analyses, and then confirms the identity of a face in a photograph or video—is one of the most powerful surveillance tools ever made. While many people interact with facial recognition merely as a way to unlock their phones or sort their photos, how companies and governments use it will have a far greater impact on people's lives.

When it's a device you own or software you use, you may be able to opt out of or turn off facial recognition, but the ubiquity of cameras makes the technology increasingly difficult to avoid in public. Concerns about that ubiquity, amplified by evidence of racial profiling and protester identification, have caused major companies, including Amazon, IBM, and Microsoft, to put a moratorium on selling their software to law enforcement. But as moratoriums expire and the technology behind facial recognition gets better and cheaper, society will need to answer big questions about how facial recognition should be regulated, as well as small questions about which services we're each willing to use and which privacy sacrifices we're each willing to make.

How facial recognition software works

Most people have seen facial recognition used in movies for decades (video), but it's rarely depicted correctly. Every facial recognition system works differently—often built on proprietary algorithms—but you can sort out the process into three basic types of technology:

Detection is the process of finding a face in an image. If you've ever used a camera that detects a face and draws a box around it to auto-focus, you've seen this technology in action. On its own, it isn't nefarious—face detection only focuses on finding a face, not the identity behind it.

Analysis (aka attribution) is the step that maps faces—often by measuring the distance between the eyes, the shape of the chin, the distance between the nose and mouth—and then converts that into a string of numbers or points, often called a "faceprint." Goofy Instagram or Snapchat filters use similar technology (video). Although analysis can suffer from glitches, particularly involving misidentification, that's generally problematic only when the faceprint is added to a recognition database.

Recognition is the attempt to confirm the identity of a person in a photo. This process is used for verification, such as in a security feature on a newer smartphone, or for identification, which attempts to answer the question "Who is in this picture?" And this is where the technology steps into the creepier side of things.

The detection phase of facial recognition starts with an algorithm that learns what a face is. Usually the creator of the algorithm does this by "training" it with photos of faces. If you cram in enough pictures to train the algorithm, over time it learns the difference between, say, a wall outlet and a face. Add another algorithm for analysis, and yet another for recognition, and you've got a recognition system.

The diversity of photos fed into the system has a profound effect on its accuracy during the analysis and recognition steps. For example, if the sample sets mostly include white men—as was the case in the training of early facial recognition systems—the programs will struggle to accurately identify BIPOC faces and women. The best facial recognition software has started to correct for this in recent years, but white males are still falsely matched less frequently (PDF) than other groups; some software misidentifies some Black and Asian people 100 times more often than white men. Mutale Nkonde, fellow of the Digital Civil Society Lab at Stanford and member of the TikTok Content Advisory Council, notes that even if the systems are operating perfectly, issues with gender identification remain: “Labels are typically binary: male, female. There is no way for that type of system to look at non-binary or even somebody who has transitioned.”

Once a company trains its software to detect and recognize faces, the software can then find and compare them with other faces in a database. This is the identification step, where the software accesses a database of photos and cross-references to attempt to identify a person based on photos from a variety of sources, from mug shots to photos scraped off social networks. It then displays the results, usually ranking them by accuracy. These systems sound complicated, but with some technical skill, you can build a facial recognition system yourself with off-the-shelf software.

A brief history of facial recognition

The roots of facial recognition formed in the 1960s, when Woodrow Wilson Bledsoe developed a system of measurements to classify photos of faces. A new, unknown face could then be compared against the data points of previously entered photos. The system wasn’t fast by modern standards, but it proved that the idea had merit. By 1967, interest from law enforcement was already creeping in, and such organizations appear to have funded Bledsoe’s continued research—which was never published—into a matching program.

In 2001, law enforcement officials used facial recognition on crowds at Super Bowl XXXV.

Throughout the ’70s, ’80s, and ’90s, new approaches with catchy names like the “Eigenface approach” (PDF) and “Fisherfaces” improved the technology’s ability to locate a face and then identify features, paving the way for modern automated systems.

Facial recognition’s first dramatic shift to the public stage in the US also brought on its first big controversy. In 2001, law enforcement officials used facial recognition on crowds at Super Bowl XXXV. Critics called it a violation of Fourth Amendment rights against unreasonable search and seizure. That year also saw the first widespread police use of the technology with a database operated by the Pinellas County Sheriff’s Office, now one of the largest local databases in the country.

Skip ahead a few years to 2008, when Illinois’s Biometric Information Privacy Act went into effect, becoming the first law of its kind in the US to regulate the unlawful collection and storage of biometric information, including photos of faces. Jennifer Lynch, surveillance litigation director at the Electronic Frontier Foundation, describes BIPA as the model for commercial regulation. “Illinois requires notice and written opt-in consent for the collection of any kind of biometric,” she says. “At this point, Illinois is the only state that requires that.”

The 2010s kickstarted the modern era of facial recognition, as computers were finally powerful enough to train the neural networks required to make facial recognition a standard feature. In 2011, facial recognition served to confirm the identity of Osama bin Laden. In 2014, Facebook publicly revealed its DeepFace photo-tagging software, the same year facial recognition played a key part in convicting a thief in Chicago and the same year Edward Snowden released documents showing the extent to which the US government was collecting images to build a database. In 2015, Baltimore police used facial recognition to identify participants in protests that arose after Freddie Gray was killed by a spinal injury suffered in a police van.

Clearview AI made news in early 2020 when The New York Times revealed that the company regularly ran its recognition software against a database of photos scraped from sources across the internet, including social media, news sites, and employment sites.

Facial recognition first trickled into personal devices as a security feature with Windows Hello and Android's Trusted Face in 2015, and then with the introduction of the iPhone X and Face ID in 2017.

Things have ramped up since then:

In 2017, President Donald Trump issued an executive order expediting facial recognition usage at US borders (and private airlines have since made their own efforts to incorporate the technology).

In 2018, Taylor Swift's security team used facial recognition to identify stalkers, and China rapidly increased its usage. Facial recognition came to Madison Square Garden as a general security measure, and retailers in the US experimented with the tech to track both legitimate shoppers and shoplifters.

In 2019, a landlord in New York tried installing it to replace keys, and several schools attempted the same.

Today, a handful of cities—San Francisco, Oakland, and Berkeley in California, plus Boston and Somerville in Massachusetts—have banned facial recognition usage by government entities. The country has also seen the first known case of a false positive leading to an arrest in the US. After Black Lives Matter police-brutality protests started in June, several large facial recognition vendors, including Amazon, IBM, and Microsoft, put a halt on selling their technology to law enforcement.

However, other, new players have entered the arena. Clearview AI made news in early 2020 when The New York Times revealed that the company regularly ran its recognition software against a database of photos scraped from sources across the internet, including social media, news sites, and employment sites—which Wirecutter, and many others, were able to confirm with testing—in a process that it used to identify suspects. In May 2020, the ACLU announced a lawsuit against Clearview AI in Illinois state court alleging that it violated the privacy rights of Illinois residents under BIPA. Clearview AI is an outlier only in that it has faced public scrutiny: Equally less ethical software companies exist—companies that will sell their software to local law enforcement, usually with no oversight or public scrutiny into where the photos come from or how the identification algorithms work.

The arguments for and against facial recognition

Proponents of facial recognition suggest that the software is useful because alongside identifying suspects, it can monitor known criminals and help identify child victims of abuse. In crowds, it could monitor for suspects at large events and increase security at airports or border crossings. The most long-running type of facial recognition software runs a photo through a government-controlled database, such as the FBI's database of over 400 million photos, which includes driver's licenses from some states, to identify a suspect. Local police departments use a variety of facial recognition software, often purchased from private companies.

There's a long list of benefits facial recognition can offer outside of law enforcement, adding convenience or security to everyday things and experiences. Facial recognition is helpful for organizing photos, useful in securing devices like laptops and phones, and beneficial in assisting blind and low-vision communities. It can be a more secure option for entry into places of business, fraud protection at ATMs, event registration, or logging in to online accounts. Advertising and commercial applications of facial recognition promise a wide array of supposed benefits, including tracking customer behaviour in a store to personalize ads online.

Brenda Leong, senior counsel and director of artificial intelligence and ethics at Future of Privacy Forum, suggested in an interview that proponents point to facial recognition as a replacement for loyalty programs or gated access: "You just walk through a set of cameras and all those things happen very seamlessly, sports arenas, event venues, amusement parks, all those places either are using or would have ideas of ways to use it similarly."

Facial recognition is helpful for organizing photos, useful in securing devices like laptops and phones, and beneficial in assisting blind and low-vision communities.

Opponents don't think these benefits are worth the privacy risks, nor do they trust the systems or the people running them. The first point of contention lies in the act of collection itself—it's very easy for law enforcement to collect photos but nearly impossible for the public to avoid having their images taken. Mug shots, for example, happen upon arrest but before conviction. Error rates in recognition are also problematic, both in a false-positive sense, where an innocent person is falsely identified, and a false-negative sense, where a guilty person isn't identified.

The facial recognition software that law enforcement agencies use isn't currently available for public audit, and the algorithms that power the detection and identification software are often closed-box proprietary systems that researchers can't investigate. When the public doesn't know how these facial recognition systems work or how accurate they are, the public doesn't know whether these systems are being used appropriately, especially in law enforcement. Joseph Flores, a software developer who in his free time uses machine learning for art projects (disclosure: I've worked on related artistic projects with Flores, for fun, not for profit), explained to me how he often intentionally biases his data sets to produce the results he wants, something law enforcement could also do: "You could do the same with your law enforcement facial recognition data to make sure that your friends were unrecognizable and your enemies were misidentified as criminals." Flores adds, "It's hard to challenge the legality or the reliability of math that you can't review. Especially with the data

scale we're talking about. With no review everything is falsifiable and just modern phrenology."

The public doesn't know whether these facial recognition systems are being used appropriately, especially in law enforcement.

Another growing issue is law enforcement's interest in real-time recognition in live video feeds or police body-cam footage. But even cities that enthusiastically moved forward with the technology, such as Orlando, Florida—where the police department used Amazon's Rekognition software to attempt to identify suspects in real time from video streams—have dialled those efforts back after the technology failed to live up to expectations. But just because real-time facial recognition still suffers from hiccups on a large scale in live testing doesn't mean it won't become widespread in the future. The idea is so appalling to some communities that the practice is already temporarily banned in California, Oregon, and New Hampshire.

The future of facial recognition and regulation

Generally speaking, the future of facial recognition can take any of three possible forms: no regulation at all, some regulation, and banning.

No regulation

The Black Mirror episodes illustrating a world devoid of facial recognition regulation write themselves. Brenda Leong provided a few examples: "It's very easy to create very Orwellian futures, where things are tracking you everywhere you go by your face because cameras are everywhere. If you're a student it could be literally watching whether you're focusing on your work versus daydreaming. If you're an employee, monitoring your engagement on your computer or telling whether you wandered off somewhere else." The list of surveillance possibilities is nearly endless, with China's "Social Credit Score" or the London police force's use of facial recognition cameras in real time offering a glimpse of one particularly grim reality.

Regulation

As of this writing, there's one proposed US law on a federal level banning police and FBI use of facial recognition, as well as another that allows exceptions with a warrant. Still another bill requires businesses to ask consent before using facial recognition software publicly, and yet another bans its use in public housing. Although facial recognition is certainly having a moment, it's still unclear which of these bills, if any, will have enough support to become laws.

When anyone talks about regulating facial recognition, they need to divide the idea into two parts: regulating commercial use and regulating government use, including that of law enforcement.

For commercial use, Leong stresses, the main thrust of regulation concerning any commercial feature—a loyalty program, theme park VIP access, or whatever else—should be consent. Facial recognition "should never be the default," she says. "It should never be part of the standard terms of service or privacy policy. And it should never be like the thing that happens that you have to then go opt out of." The easiest way to see how such

regulation might work in practice on a federal level is to look at Illinois's BIPA, which requires consent before an entity can collect and use biometric data (including faceprints) and imposes requirements upon the storage of that data.

The list of surveillance possibilities is nearly endless

Consent can be tricky, though. It's one thing for a store to ask if you want to skip showing your ID to enter and another when the store uses this technology to track shoplifters across all its franchise locations. As an example, the EFF's Jennifer Lynch points to a recent case of a business district in London where a company placed cameras in a privately run area that people who worked nearby passed through: "You could see that the business district might say, 'Oh, well, we put up signs,'" Lynch says. "And so people know that when they walk in this area or their face is being recorded and captured, but I don't really believe that people can actually meaningfully consent in that situation. If you are working in that area, you may not have a choice of working somewhere else."

When it comes to the government's use of facial recognition, suggested policy approaches diverge. Leong says that although Future of Privacy Forum's main focus is on commercial use of facial recognition, the group would want to see regulation of government use, too. "We would very much like to see overt, intentional regulatory guidance around how the government can and should use facial recognition," she says, "even if it's just things like being really clear about what levels of warrant or probable cause are required for agencies to access it."

Other groups, including the EFF, don't think regulation of law enforcement can go far enough.

Banning

Lynch, along with the EFF, argues that regulation isn't sufficient. "We are pushing for a ban or at least a moratorium at the federal, state, and local level on government use of face recognition," Lynch says. "It is a really game-changing technology and I think we're at a key point in history where we could prevent broad government use of face recognition."

Even as facial recognition addresses its diversity problem, there are still too many potential issues concerning how it's used. "The security and policing industries are predicated on this idea that Black people are dangerous," Mutale Nkonde says. "And so when thinking about tools for policing or tools for security, there is going to be this disproportionate deployment against Black people." That is why Nkonde supports banning the software's use outright: "I would want to see a ban around human subjects, just because I think the privacy trade-offs are too huge."

Privacy tips for using everyday things with facial recognition

Although policy changes, whether in the form of regulation or bans, offer the clearest way forward on a national scale, enacting such changes takes time. Meanwhile, there are smaller but not insignificant ways people interact with facial recognition on a daily basis that are worth thinking deeply about.

"I think that the concerning thing and the place where the distinctions sort of blur is that the more we use face recognition, the less we start to think of it, the less we think of it as risky

out in the world, we become accustomed to it," says Lynch. "I think it's a slippery slope from using face recognition on your phone to the government using face recognition to track us wherever we go."

What about facial recognition in Google Photos or Apple Photos? Photo organization was the first time many people saw facial recognition in action. Apple has made a big show of describing how its facial recognition data in Photos runs on the device (PDF). This technology is more private than a cloud server, but it is also less accurate than cloud-based software. Face grouping in Google Photos can be very accurate, but Google's wide array of services and devices means the company tends to share data liberally across the services it provides. In 2016, Google was sued in Illinois for its use of facial recognition, but that suit was later dismissed. In 2020, a new class action suit alleges a similar offense. Although the ability to organize photos by faces using the facial recognition feature in a photos app offers quantifiable benefits, there is a privacy trade-off to consider. It's difficult to know exactly how a company might misuse your data; this was the case with the photo storage company Ever, whose customers trained the Ever AI algorithm without realizing it. You can disable face grouping in Google Photos. You can't turn the corresponding feature off in Apple's Photos app, but if you don't actively go in and link a photo to a name, the recognition data never leaves your device.

What about Facebook? Facebook likely has the largest facial data set ever assembled, and if Facebook has proven anything over the years, it's that people shouldn't trust the company to do the right thing with the data it collects. Facebook recently agreed to pay $550 million to settle a lawsuit in Illinois over its photo tagging system. Here's how to opt out.

What about unlocking a phone or computer? As the features work now, face unlock typically happens only on the device itself, and that data is never uploaded to a server or added to a database.

What about facial recognition in home security cameras? The systems behind security cameras lack clear consent as they record and opt-in people automatically, often in defiance of local privacy laws, an ethical problem many people neglect to consider. Right now, only a handful of home security cameras include facial recognition, including Wirecutter's smart doorbell upgrade pick, Google's Nest Hello. Face detection on Nest cameras is off by default, however. More worrisome to privacy advocates is the potential inclusion of facial recognition with Ring cameras, a system that shares data with police through its Neighbours app.

Do you need to worry about those goofy face apps that pop up once a year or so? The most recent app to break through in this arena was FaceApp, which gained popularity by allowing people to age themselves. Although the company says it doesn't use the app to train facial recognition software, it's difficult to know what might happen with the data the app collects if the company gets sold. The same goes for whatever the next version of FaceApp is. It's best to be wary of this type of software.

Can facial recognition identify you if you're wearing a mask? It's not likely right now but may be in the future. One company in China was able to get facial recognition working on 95% of mask wearers, but this specific software was designed for small-scale databases of around 50,000 employees. Companies are scrambling to solve this problem.

Where society goes from here promises to be a mixture of policy and tweaks to people's personal habits, but the conversation concerning the technology likely isn't going anywhere for a long time. Like any technology, facial recognition is itself just software, but as Mutale Nkonde notes, how society uses it is what matters: "It's the way the tool impacts our civil and human rights that is my point of intervention, because I think that all technology is agnostic."

'The Pros and Cons of Facial Recognition Technology' (D Gargaro, *ITPro.com*, 20 July 2021)

Once seen as the symbol of advancement in future civilisations, especially in sci-fi staples such as Star Trek or 2001: Space Odyssey, facial recognition has quickly become a mainstream component of our day-to-day life. From unlocking our mobile devices to tagging our friends in Facebook posts, this type of biometric technology makes authentication quick, simple, and (most of the time) accurate.

However, facial recognition has also been the subject of plenty of controversies, especially in the aftermath of the shooting of George Floyd, which drew attention to the racially motivated police brutality in the US. Due to many police forces relying on facial recognition technology to identify potential suspects, tech giants such as Amazon, Microsoft, and IBM had chosen to reconsider their stances on its development and sales. Weeks later, the use of facial recognition for law enforcement purposes was also deemed unlawful in the UK, with the Court of Appeal declaring that the technology violates human rights, data protection laws, and equality laws.

The topic is also expected to be debated in the European Parliament, with policymakers being asked to ban the use of facial recognition as a biometric mass surveillance tool. A petition launched by a coalition of privacy advocates which warns of numerous potential outcomes of not regulating the technology has so far been signed by 42,489 people.

Nevertheless, facial recognition is still being used in a number of other scenarios, including the workplace, where at times it's trusted with making decisions such as hiring – or firing – employees.

Wherever it's being used, facial recognition is likely to attract a lot of attention. That is why we've collated a list of pros and cons related to facial recognition so that you can stay informed on this controversial topic.

Pros of facial recognition

There are many benefits facial recognition can offer society, from preventing crimes and increasing safety and security to reducing unnecessary human interaction and labor. In some instances, it can even help support medical efforts.

<u>Helps find missing people and identify perpetrators</u>

Law enforcement agencies use facial recognition to identify criminals with no other means of identification and find missing people by comparing faces on live camera feeds with those on a watch list.

They've also used it to find missing children, combining facial recognition with ageing software to predict how children would look several years on and find them even when they've been missing for years. Police receive live alerts and are able to investigate potential matches in real-time.

Protects businesses against theft

Facial recognition software can be an effective pre-emptive measure against shoplifting. Business owners use the software and security cameras to identify known or suspected thieves, and the presence of the cameras themselves work to deter theft in the first place.

If a business does end up getting stolen from, the software can also help identify and track the thieves.

Strengthens security measures in banks and airports

Facial recognition also helps improve safety and security in non-retail spaces, like airports and banks.

It's been a regular part of airport security screening for years. Similar to identifying criminals that come into shops, the software has helped identify criminals and potential threats to airlines and passengers.

The US Customs and Border Protection (CBP) has promised to use facial recognition on 97% of international passengers by 2023.

An additional benefit is that it runs border checks much more quickly and accurately than people can.

Institutions like banks use the software in the same way to prevent fraud, identifying those previously charged with crimes and alerting the bank so they know to pay extra attention to the person's business at the bank.

Air travellers pass through automated passport border control gates at Heathrow Airport, where the UK Border Force uses facial recognition technology.

Makes shopping more efficient

While identifying and finding missing persons and criminals are arguably the most important benefits of facial recognition, they extend beyond security to convenience.

Instead of making cash or credit purchases at stores, facial recognition technology can recognize your face and charge the goods to your account.

Use of this increased during the pandemic to serve both convenience and security purposes, as well as help manage the smaller ratio of staff to customers, but retailers also see the tech being used in the future to recognise and advertise to loyalty club members and clock employees in and out.

Reduces the number of touchpoints

Facial recognition requires fewer human resources than other types of security measures, such as fingerprinting. It also doesn't require physical contact or direct human interaction. Instead, it uses AI to make it an automatic and seamless process.

It also limits touchpoints when unlocking doors and smartphones, getting cash from the ATM or performing any other task that generally requires a PIN, password or key.

Improves photo organization

Facial recognition can also tag photos in your cloud storage through Apple or Google. This makes it easier to organize, find and share your photos. It also plays a role in suggesting tags on Facebook.

Improves medical treatment

One surprising use of facial recognition technology is the detection of genetic disorders.

By examining subtle facial traits, facial recognition software can, in some cases, determine how specific genetic mutations caused a particular syndrome. The technology may be faster and less expensive than traditional genetic testing.

Cons of facial recognition

As with any technology, there are potential drawbacks to using facial recognition, such as threats to privacy, violations of rights and personal freedoms, potential data theft and other crimes. There's also the risk of errors due to flaws in the technology.

Threatens individual and societal privacy

The threat to individual privacy is a significant downside of facial recognition technology. People don't like having their faces recorded and stored in a database for unknown future use.

Privacy is such a big issue that some cities, including San Francisco, California and Cambridge, Massachusetts, have banned law enforcement's use of real-time facial recognition surveillance. In these cases, police can use video recordings from personally owned security video devices, but they can't use live facial recognition software.

Imposes on personal freedom

Being recorded and scanned by facial recognition technology can make people feel like they're always being watched and judged for their behaviour. Plus, police can use facial recognition to run everyone in their database through a virtual criminal line-up, which is like treating you as a criminal suspect without probable cause.

Violates personal rights

Graphic of a gigantic and sinister CCTV camera observing anonymous people in a crowd

Countries with limited personal freedoms, such as China, UAE, North Korea, Iran and Iraq, commonly use facial recognition to spy on citizens and arrest those deemed troublemakers.

Creates data vulnerabilities

There is also concern about the storage of facial recognition data, as these databases have the potential to be breached.

Hackers have broken into databases containing facial scans collected and used by banks, police departments and defense firms in the past.

Provides opportunities for fraud and other crimes

Lawbreakers can use facial recognition technology to perpetrate crimes against innocent victims too. They can collect individuals' personal information, including imagery and video collected from facial scans and stored in databases, to commit identity fraud.

With this information, a thief could take out credit cards and other debt or open bank accounts in the victim's name, or even build a criminal record using the victim's identity.

Beyond fraud, bad actors can harass or stalk victims using facial recognition technology.

For example, stalkers could perform reverse image searches on a picture taken in a public place to gather information about their victims and determine who they are and where they live.

Plus, because technological crime moves faster than the law, people can be victimized before the activity is viewed as a crime.

Technology is imperfect

Facial recognition isn't perfect. For example, it's less effective at identifying women and people of colour than white males.

The technology depends upon algorithms to make facial matches. Those algorithms are more robust for White men than other groups because the databases contain more data on White men than women and people of colour. This creates unintentional biases in the algorithms.

Innocent people could be charged

There are inherent dangers in false positives. Facial recognition software could improperly identify someone as a criminal, resulting in an arrest.

This issue is exasperated when you add that the technology struggles with people of colour, which increases the potential for racial profiling accusations.

Technology can be fooled

Other factors can affect the technology's ability to recognize people's faces, including camera angles, lighting levels and image or video quality. People wearing disguises or slightly changing their appearance can throw off facial recognition technology too.

Technology continues to evolve

As facial recognition technology improves, its challenges will decrease. Other technology could impact its effectiveness, including recognizing body parts or how a person walks.

For the time being, though, the technology's inadequacies and people's reliance on it means facial recognition has room to grow and improve.

'Home Quarantine Apps Spark Privacy Fears Over Facial Recognition and Geolocation Technology' (J Taylor, *The Guardian Australia*, 13 October 2021)

Apps used to ensure overseas arrivals are complying with home quarantine requirements as part of Australia's opening up need stronger privacy protections, technology and human rights groups have told state and federal health ministers.

As Australia starts opening up to the rest of the world again, states are moving to adopt home quarantine as a less expensive alternative to the hotel quarantine system.

South Australia is the only jurisdiction actively trialling home quarantining technology using a government-built app called Home Quarantine SA. The app randomly alerts users to verify their location and send a selfie back to authorities within 15 minutes to prove they are at the home they have registered to quarantine at.

As of Wednesday, 141 people had completed the SA trial, with 171 enrolled. Six had pulled out of the trial – two of whom withdrew due to issues using the app. SA Health said so far there had been 100% compliance with the testing schedule and symptom checking.

The Human Rights Law Centre and Digital Rights Watch have written to the health ministers in each state and territory, as well as the federal health minister, Greg Hunt, expressing concern about the use of facial recognition technology and location information without stronger privacy protections in place.

The groups say using facial recognition technology is “an extreme measure” given human rights organisations globally, including the Australian Human Rights Commission, have called for a moratorium on its use without a strong regulatory framework in place, due to concerns such as racial bias.

“We are concerned that a significant proportion of users of such home quarantine apps may face unreasonable technical barriers to effectively use the tool through no fault of their own,” the letter states. “It is unacceptable to subject individuals to the consequences of not meeting requirements to ‘check in’ if they are unable to do so as a result of the technology exhibiting racial bias.”

The letter also raises concern that although the data is encrypted on submission and stored on an Australian server, information will not be destroyed until “the conclusion of the Covid-19 pandemic unless required for enforcement purposes for any alleged breach of a direction by you under the Emergency Management Act 2004.”

The groups argue there is no reason for the data to be retained longer than the home quarantine period, and it is unknown when the pandemic will be over. There is also concern law enforcement agencies may try to access the data for the investigation of unrelated crimes, similar to attempts to access QR code check-in data.

“Without robust and specific protections in place, the information collected by home quarantine apps may later be used for secondary purposes unrelated to public health,” the letter states. “This risks undermining support and compliance, and ultimately compromising the public health response.”

A spokesperson for the South Australian Department of the Premier and Cabinet said the app “collects and uses the minimum amount of personally identifiable information” to enable compliance with the home quarantine requirements.

“The Home Quarantine SA app facial verification technology can be used by people of any age, ethnicity, gender or cognitive ability,” the spokesperson said.

Although the Covidsafe contact tracing app largely proved unhelpful in detecting close contacts during outbreaks in Australia, the groups said the extensive privacy legislation passed to support the app – including limiting access to the data by law enforcement – was something the states should adopt for home quarantine apps.

“The information collected by the home quarantine app, as well as that collected via QR ‘check ins’, is no less sensitive to that which was to be collected by the Covidsafe app,” the Digital Rights Watch program lead, Samantha Floreani, said.

The Human Rights Law Centre senior lawyer Kieran Pender said one measure that should be considered is for all biometric and location verification to be done on the phone itself, rather than being transferred to a government server.

"That would be a more secure approach that would still permit the necessary verification to take place," he said.

A spokesperson for the federal health minister directed questions about privacy requirements for the apps to the attorney general, Michaelia Cash. A spokesperson for Cash said the home quarantine arrangements were a matter for the states that managed them.

On Tuesday, the South Australian auditor general revealed in a report on the state's QR code app that the SA Department of the Premier and Cabinet, which is responsible for the app, had retained check-in data beyond the 28 days the government had said the records would be retained.

The records were retained as part of the department's regular department-wide back-up of data, and DPC advised the auditor general the backups had controls to prevent unauthorised restoration, and if the data was restored, it would automatically delete being over 28 days old.

'Microsoft Agrees to Human Rights Review of Deals with Law Enforcement and Government' (D Bass, *Time Magazine/Bloomberg*, 13 October 2021)

Microsoft Corp., which has faced pressure from employees and shareholders over contracts with governments and law enforcement agencies, agreed to commission an independent human rights review of some of those deals.

The move came in response to a June filing of a shareholder proposal asking the company to evaluate how well it sticks to its human rights statement and related policies. Microsoft committed to a review of any human rights impacts that its products have on those including communities of Black, Indigenous and People of Color in contracts for police, immigration enforcement and unspecified other government agencies, according to correspondence from the company viewed by Bloomberg.

Microsoft pledged to publish the report next year, and the shareholders, who include faith-based investors like Religious of the Sacred Heart of Mary, have withdrawn their proposal ahead of Microsoft's annual shareholder meeting next month.

Microsoft spokesman Frank Shaw confirmed the company will undertake the review.

"In response to shareholder requests, Microsoft Corp. will commission an independent, third-party assessment to identify, understand, assess, and address actual or potential adverse human rights impacts of the company's products and services and business relationships with regard to law enforcement, immigration enforcement, and other government contracts. The assessment will include consultation with BIPOC communities, including immigrants, and other groups representing communities most impacted by Microsoft's surveillance products, law enforcement and government contracts," the company said in a statement.

As government, military and police contracts have become targets of scrutiny and activism, Microsoft employees have circulated letters demanding the company abandon a deal to build versions of its HoloLens augmented reality headsets for the U.S. Army as well as raising concerns about business with U.S. Immigration and Customs Enforcement. Chief Executive Officer Satya Nadella has stood behind software sales to the U.S. military, but paused selling facial recognition technology to police departments, although the company sells other programs to law enforcement. The California-based religious order agreed to lead the shareholder proposal because it wanted to make sure the company's products don't

“cause human rights harms, including perpetuating systemic racial inequities,” Sister Joanne Safian, said in a statement.

Microsoft told the investors the review will be conducted by the law firm Foley Hoag LLP. The proposal was filed by Investor Advocates for Social Justice, a nonprofit representing faith-based institutional investors. Microsoft didn’t specify which contracts will be examined, but shareholders “expect” it will include what the group said are about 16 active contracts with ICE and U.S. Customs and Border Protection.

“This will be an ambitious and complicated process and we’re certainly putting our faith in Microsoft and Foley Hoag to be conscientious,” said Michael Connor, executive director of Open MIC, a nonprofit shareholder advocacy organization that worked with IASJ on the proposal. “They’re asking for input from affected rights holders, which was a very big request on our part and they agreed to that.”

Human rights concerns have been raised by shareholders in areas related to labor and in the apparel industry around manufacturing conditions but are newer to the technology companies, he said. Open MIC has also made similar requests of Amazon.com Inc., related to its facial recognition technology, as well as Apple Inc., Facebook Inc. and Alphabet Inc., without a positive response from the companies or a win at shareholder meetings, Connor said.

Open MIC is also working on two other shareholder resolutions related to Microsoft, including one that asks the company to stop selling facial recognition software to all government agencies.

“Tech companies take the position that all tech is good, and while we as shareholders recognize that tech can be helpful, there are also many downsides,” Connor said.

Microsoft earlier this month agreed to let more repair shops fix its devices in response to a push from As You Sow, a nonprofit shareholder activism group, and consumer advocates.

KNOX GRAMMAR SCHOOL

DA VINCI DECATHLON 2021

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS

IDEATION – ANSWER BOOKLET

TEAM NUMBER _____

1	2	3	4	Total	Rank
/15	/10	/25	/10	/60	

IDEATION CHECKLIST

To ensure that your team is on track and has completed all of the required tasks for the challenge please note the following checklist.

TASKS	COMPLETE – PLEASE TICK
a. Empathise - Research form (15 marks)	
b. Define (10 marks)	
c. Ideate (25 marks)	
d. Prototype (10 marks)	

Team Code: _____

1. EMPATHISE

What is the problem?

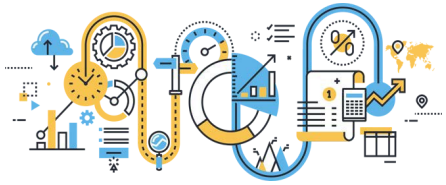
- Define the challenge and explore the human context (15 marks)

Research is imperative when identifying problems and solutions. Without knowledge of the context and consideration of the human context, it can be very difficult to identify a problem or challenge on which you will focus.

This section will guide you through an examination of the research material that has been provided for this topic.
In the box below, identify what you consider to be **KEY FACTS** from the research provided. Use the headings to guide your research.

Factors contributing to the issue (At least TWO) – 4 marks	**Consequences if not addressed (At least TWO) – 4 marks**	**People and perspectives – Identify the different perspectives – 3 marks**	**Two barriers to addressing the issue and why they are a barrier – 4 marks**

2. DEFINE



Why is it important? (10 marks)

- Understand and create a point of view

The consideration of ethics distinguishes us as humans from other organisms. Ethical people have what philosopher Thomas Aquinas called a *'well-informed conscience'*. They live what Socrates called *'an examined life'* – a life particularly associated with being human. Here, you must identify the problem in a vision statement. This is your team's vision for what you would like to achieve. It may be that you want to 'reduce' or 'improve', 'increase' or decrease'.

Vision Statement: What does the team want to achieve? (5 marks)

Why is this vision statement important to address? Write the relevant points from the research here to show you have based your vision statement on your understanding of the problem. (5 marks)

Team Code: _____

3. IDEATE

How do we solve it? (25 marks)

Create **3 POSSIBLE** solutions that will facilitate your vision statement. In other words, how will you make this a reality? They need to be **3 DIFFERENT** ideas. Be bold, be creative.

Possible Solution 1 (2 marks)	**Possible Solution 2 (2 marks)**	**Possible Solution 3 (2 marks)**
Reflect and Evaluate: complete this once you have brainstormed your solutions		
What are some positive consequences of this solution? (1 mark)	*What are some positive consequences of this solution?* (1 mark)	*What are some positive consequences of this solution?* (1 mark)
What are some negative consequences of this solution? (1 mark)	*What are some negative consequences of this solution?* (1 mark)	*What are some negative consequences of this solution?* (1 mark)

Team Code: _____

REFLECT & EVALUATE Cont.

Using the table above, select one solution for which you will develop a prototype.

Write your chosen solution here (2 marks)

Justify why you have selected this solution (4 marks)

IMPLEMENTATION (3 marks)

WHEN?

WHERE?

WHO?

DISSEMINATION (4 marks)

How will you get people to adopt your idea?

How will you measure your success?

Team Code: _____

4. CREATE

PROTOTYPE (10 MARKS)

A prototype is a simple experimental model of a proposed solution used to test or validate ideas, design assumptions and other aspects of its conceptualisation quickly and easily. Please create a mindmap or a storyboard or poster as a model of your solution on the following pages.

ASPECT	LIMITED	SOUND	EFFECTIVE	OUTSTANDING	MARK
Originality and creativity	0 - 1	2-3	4	5	
Clarity and communication of ideas	0 - 1	2-3	4	5	
				TOTAL	/10

PROTOTYPE

PROTOTYPE

END OF PAPER