|  | **Explore PT - Response 2d - All Samples** |  |
| --- | --- | --- |

**2d**. Using specific details, describe:

* the data your innovation uses;
* how the innovation consumes (as input), produces (as output), and/or transforms data; and
* at least one data storage concern, data privacy concern, or data security concern directly related to the computing innovation.

*(Must not exceed 250 words)*

| **Scoring Guidelines** |
| --- |
| **Row and Task** | **Decision Rules** |
| **Row 6****Response 2D**● Identifies the data that the identified or described computing innovation uses AND ● Explains how that data is consumed, produced, OR transformed. | Responses should be evaluated on the rationale provided in the response not on the interpretation or inference on the part of the scorer. **Do NOT award a point if any one of the following is true:** * the described innovation is not a computing innovation; or
* the response does not state the specific name of the data or simply says “data”; or
* the response confuses or conflates the innovation with the data: response fails to explain what happens to the data; or
* the response confuses the source of the data with the data.
 |
| **Row 7****Response 2D**● Identify one data storage, data privacy, OR ● data security concern related to the identified or described computing innovation. | Responses should be evaluated on the rationale provided in the response not on the interpretation or inference on the part of the scorer. Responses can earn this point even if they refer to the data in a general without specifically identifying the data being used.**Do NOT award a point if any one of the following is true**: * the described innovation is not a computing innovation; or
* the response identifies or describes a concern that is not related to data
 |

| **Student Response A - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-a-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-a-written.pdf)**]** | **Scoring Guidelines** |
| --- | --- |
| The system of blockchain operates with a distributed ledger. According to Coindesk, “a distributed ledger is a database held and updated independently by each participant (or node) in a large network.” (Bauerle)The computers use metadata from transaction requests. Each block of data contains a pointer to the previous block, a timestamp, and transaction data. Then, this chain of blocks is held in the storage of each node. The data it produces is the blockchain itself, which is a stream of transaction data separated into blocks by set intervals of time. This data is kept in a ledger, which does not need to be verified by a central authority. (Siegel) It computes by taking the data and runs it through algorithms to verify the identity of the request. “In the case of blockchain technology, private key cryptography provides a powerful ownership tool that fulfills authentication requirements. Possession of a private key is ownership.” (Bauerle). So essentially, the blockchain computes by running transaction data through algorithms that verify private key ownership. A privacy concern is that “Bitcoin relies on a public blockchain, a system of recording transactions that allows anyone to read or write transactions. Anyone can aggregate and publish those transactions, provided they can show that a sufficient amount of effort went into doing so.” (Berke) This means that anyone who really wanted to could see transactions being made on the blockchain, and with a little effort and computing ability, they’d have access to transaction amounts, time, and other data | **Row 6** | **1** |
| **The response earned a point for this row.** The response identifies the data: "Each block of data contains a pointer to the previous block, a timestamp, and transaction data." It then states that "It computes by taking the data and runs it through algorithms to verify the identity of the request," which describes how the data is consumed. |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response earned the point for this row. The response identifies the privacy concern: "Bitcoin relies on a public Blockchain, a system of recording transactions that allows anyone to read or write transactions." |
| **Student Response B - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-b-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-b-written.pdf)**]** | **Scoring Guidelines** |
| Virtual reality uses image, motion, orientation, and distance data to operate (Mullis). All this data is consumed by the headset to allow the headset to detect user input and its surroundings. This data is then transformed by the program running on the headset to determine what to show the user and is outputted to the user in the form of image and audio data. A data privacy concern associated with virtual reality is the potential ability for companies to access the video or other sensor data recorded by these headsets, which could be used for things without your consent. Since the headset has seen where one has been walking or driving, someone else with access could also see this and may have the ability to find them against his/her will. | **Row 6** | **1** |
| **The response earned a point for this row.** The response identifies the data as "image, motion, orientation, and distance." The response explains how the data is consumed: "All this data is consumed by the headset to allow the headset to detect user input and its surroundings. This data is then transformed by the program running on the headset to determine what to show the user and is outputted to the user in the form of image and audio data." |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response identifies a data privacy concern: " the potential ability for companies to access the video or other sensor data recorded by these headsets, which could be used for things without your consent." It goes on to say, "someone else with access could also see this and may have the ability to find them against his/her will."  |
| **Student Response C - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-c-artifact.mp4)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-c-written.pdf)**]** | **Scoring Guidelines** |
| When adding a new card to the digital wallet, Apple creates a Device Account Number in place of the credit card number that is stored with the bank, on the device, and on Apple’s servers, and then erases the credit card number from its database. When paying with Apple Pay, the paying device transmits the user’s Device Account Number over an encrypted NFC connection to the terminal. The Device Account Number is then sent to the bank and verified [1]. Although Apple Pay does allow increased security, it does have its own security concerns. When registering a new card on an unsecured public Wi-Fi network, a cybercriminal can spoof a user’s mobile wallet registration system in which the user must enter their card’s data. Malware is also a security concern as it can be used to steal credit card information [3].  | **Row 6** | **1** |
| **The response earned a point for this row.** The response identifies data by stating that "Apple creates a Device Account Number in place of the credit card number that is stored with the bank, on the device, and on Apple's servers, and then erases the credit card number from its database." The response explains how data is output from the device in that "When paying with Apple Pay, the paying device transmits the user's Device Account Number over an encrypted NFC connection to the terminal. The Device Account Number is then sent to the bank and verified." |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response identifies a data security concern by stating that "When registering a new card on an unsecured public Wi-Fi network, a cybercriminal can spoof a user's mobile wallet registration system in which the user must enter their card's data." |
| **Student Response D - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-d-artifact.mp4)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-d-written.pdf)**]** | **Scoring Guidelines** |
| The Microsoft HoloLens inputs data by using different types of cameras, microphones, and a light sensor [7]. Then, the Holographic Processing Unit and Central Processing Unit takes in the data captured by the cameras, microphones, light sensor and transforms those data by projecting images onto the lens in the correct position in the device, creating the realistic 3D holographic image that the users see [1]. One of the data security concern is that the data captured by the cameras and the sensors may be altered by a malicious program on the device, making the device’s Central Processing Unit and Holographic Processing Unit output realistic altered holographic images like a huge insect to suddenly scare the user and altering human facial features with holograms tricking the user into identifying people incorrectly when wearing the device [4]. | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** The response does not identify the data, but rather lists data collection devices such as "cameras, microphones, and a light sensor." |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response identifies a data security concern as "the data captured by the cameras and the sensors may be altered by a malicious program on the device, making the device's Central Processing Unit and Holographic Processing Unit output realistic altered holographic images." |
| **Student Response E - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-e-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-e-written.pdf)**]** | **Scoring Guidelines** |
| Bitcoin uses a hash generation system which leads users to unlock hatches. The hash is a randomly generated code that increases difficulty the more hatches that are opened. The user must generate this code before opening a hatch and receiving a reward in Bitcoin. The system of mining is a hard hobby to break into because of the difficulty of hashes now. The system puts out an output which is the randomly generated hash and the user must test many hashes before they ultimately guess the exact hash that the system created [4, 1]. A data privacy concern includes the user’s names. There is a large ledger that is kept on an open server that can only be changed by transactions. A user makes an account and a username that will be seen on the transaction ledger. This ledger will include every transaction ever made with a Bitcoin. This ledger tracks every Bitcoin ever found and shows which users are in possession of them. The ledger also Explore Sample E 1 of 12 shows which user lost the Bitcoin and which user gained the Bitcoin in the transaction. The ledger is text but has a file size near 2 gigabytes [4]. The storage of this ledger is not a concern, nor is the security because of the level of encryption on the ledger itself. Privacy is an issue because there was a discovery of the federal government using Bitcoin to make transactions on the black market [4, 1]. The privacy of users rises an issue within the community. | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** The response does not identify the data and explain how that data is consumed, produced, or transformed. The response describes how Bitcoin functions rather than the data and its use of the data. |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response raises a data privacy concern that username data is maintained on "a large ledger that is kept on an open server that can only be changed by transactions. A user makes an account and a username that will be seen on the transaction ledger. This ledger will include every transaction ever made with a Bitcoin." |
| **Student Response F - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-f-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-f-written.pdf)**]** | **Scoring Guidelines** |
| Data is necessary for social media in an economic standpoint. First off, this innovation consumes knowledge based on what it learns. A majority of businesses with successful social media presence, utilize some sort of social listening, which are analytics tools that constantly gather useful customer data and track conversations about target brands or themes(2). Therefore the person who is being interviewed must tell them the necessary information in which the business will consume the data and see if that person will fit in well with their business. While this data may be useful to some, there can also be concerns for breach of data. If some people don’t take actions on their privacy, such as sharing their profiles to the rest of the world, then they may allow other people to find out personal information about them such as gender, where they live, how old they are, and other possible information. This can be harmful to that person as someone who is unknown to them, will know a lot about them.  | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** The response does not identify data that the innovation uses, rather it simply states that "data is necessary," nor how it is consumed, transformed, or output. |
| **Row 7** | **1** |
| **The response earned a point for this row.** The response does identify a concern "for breach of data" in that "If some people don't take actions on their privacy, such as sharing their profiles to the rest of the world, then they may allow other people to find out personal information about them such as gender, where they live, how old they are, and other possible information." |
| **Student Response G - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-g-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-g-written.pdf)**]** | **Scoring Guidelines** |
| These prosthetics utilizes myoelectric signals to simply activate mechanical motors in a prosthetic appendage. These prosthetics simply consumes the electromyographic data sent to specific muscles on the user's body from the brain. This data is received through the EMG sensors that are attached to the proper muscles on the wearer. These EMG signals, once received, are transmited to a signal processor that identifies which sensor is transmitting a signal then appropriately actuates a combination of cervos and motors in order to properly move the prosthetic as if an appendage was there. | **Row 6** | **1** |
| **The response earned a point for this row.** The response identifies the data as myoelectric signals. The response explains how the data is consumed: "These prosthetics simply consumes the electromyographic data sent to specific muscles on the user's body from the brain. This data is received through the EMG sensors that are attached to the proper muscles on the wearer. These EMG signals, once received, are transmitted to a signal processor that identifies which sensor is transmitting a signal then appropriately actuates a combination of cervos and motors in order to properly move the prosthetic as if an appendage was there." |
| **Row 7** | **0** |
| **The response DID NOT earn a point for this row.** The response does not identify a concern that is related to the data. |
| **Student Response H - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-h-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-h-written.pdf)**]** | **Scoring Guidelines** |
| The data that iphone x use is mobile data. Iphone x consumes as input as that there is touch screen, apps, games, etc and produces as output as that it uses audio, voice, power, etc. The iphone x’s uses lots of data for the new feature, face ID. The data Explore Sample H 2 of 4 from the infrared camera is sent to A11 chip to process, in which it compare the information about you on the phone(5). Apple has analyzed over a billion images for data about faces(5). One of the data storage concern is that the there is limited space to store files for example, pictures and videos have bigger size because of improved cameras, so it require more data to store. The face ID has some security concerns, someones can crack the Face ID with a composite mask of 3-D-printed plastic, silicone, makeup, and simple paper cutouts, which in combination trick an iPhone X into unlocking (6). So there is concern about the security of face ID on iphone x.  | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** The input data is not identified. The response does mention audio and voice as output, which would be produced by the phone, not used by the phone. |
| **Row 7** | **1** |
| **The response earned a point for this row.** A security concern is identified: "The face ID has some security concerns, someones [sic] can crack the Face ID with a composite mask of 3-D printed plastic, silicone, makeup, and simple paper cutouts, which in combination trick an iPhone X into unlocking" |
| **Student Response I - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-i-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-i-written.pdf)**]** | **Scoring Guidelines** |
| This Apple watches you can send messages, call, go underwater, and see your health. Apple watch gets its data from wifi and Bluetooth and also from the iPhone. Data is sending things to people and using it. The Apple watch use 16gb. An input is “Siri feels more useful, and Apple music streaming not ready yet.” A transform is “it's a great gift, and you can use it if you don’t have your phone.” A produce is It can work with you all day long and helps you around. An Apple watch computes by “The Apple Watch Series 3 with cellular takes a major step forward in making Apple's wrist-worn device its own independent, connected computing platform.” The Apple watch is storage and privacy. It’s storage because you only have 16gb, you can only that much and no more. It’s privacy because it's like your phone, you don’t want anyone to go through your phone to see your message, photos, apps, and more. So, your Apple watch is private too so only you can use it and see what’s on it.  | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** The response does not specify the specific name of the data but rather just refers to it as data. |
| **Row 7** | **0** |
| **The response DID NOT earn a point for this row.** The response identifies storage size of the computing innovation and access to your device, but these are not related to the data. |
| **Student Response J - [**[**Artifact**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-j-artifact.pdf)**] [**[**Written Response**](https://secure-media.collegeboard.org/ap/video_audio/ap18-explore-sample-j-written.pdf)**]** | **Scoring Guidelines** |
| The Human Genome Project uses approximately 1 zetta-base per year. The innovation acquires data from highly distributed sources such as universities, hospitals, and research laboratories. There are currently more than 2,500 sequencing instruments made by different manufacturers that are distributed throughout different nations.The resulting big data is distributed in units as a few genetic comparisons or gene sequences or as bulk downloads from from central repositories. To reduce the computing resources necessary for large-scale analysis of the data, cloud computing is used so that only small sections of code are uploaded and highly processed data are downloaded. The data for genomics is enormous, and it’s estimated that up to 40 exabytes will be needed by 2050. Efficient data compression is one solution but decompression time is also a concern. The data is medically sensitive information and must be carefully guarded. Homomorphic encryption can be used to allow only certain groups to view the data, but it is currently too expensive[2].  | **Row 6** | **0** |
| **The response DID NOT earn a point for this row.** It is unclear whether the data that has been identified is connected to a computing innovation. |
| **Row 7** | **0** |
| **The response DID NOT earn a point for this row.** Even though cloud computing is a computing innovation and mentioned in this prompt, it is unclear how this is connected to the data storage concerns. |