Stage Two Questionnaire

The explanation sentences using different principles have been highlighted. For each question, the correct answers are highlighted. Each question has more than one correct answer.

1. Policy Snippet: "*We collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and* ***biometric data****). Nor do we collect any information about criminal convictions and offences.*"

Domain-specificity:
Biometrics are biological measurements or physical characteristics that can be used to identify individuals, **for example, fingerprint, palm print and face recognition. Additionally, behavioral characteristics are related to the pattern of behavior of a person, like mouse movement, speaking rhythm and behavioral profiling.**

Implication-oriented:
Biometrics are biological measurements or physical characteristics that can be used to identify individuals. **The Skill may use such data to enable some functionalities with your consent. Your biometric data is forever linked to your identity and you cannot change it. So, once it is leaked or compromised, you are at continual risk of identity-based attacks.**

After reading the above Alexa Skill policy snippet, which answers do you think are correct regarding "**biometric data**" in relation to this Alexa Skill?
1. The Skill may collect your IP address if they collect your biometric data.
2. The Skill may collect your heart rate if they use the related sensor.
3. The attacker may create a fake voice ID to open your Alexa Device if your biometric data is stolen.
4. The attacker may know your home address if your biometric data is stolen.

2. Policy Snippet: "*The Service uses the following types of cookies for the purposes set out below:* ***Essential Cookies****: These cookies are essential to provide you with services available through the Service and to enable you to use some of its features. For example, they allow you to log in to secure areas of the sites or applications and help the content of the pages you request load quickly. Without these cookies, the services that you have asked for cannot be provided, and we only use these cookies to provide you with those services.*"

Domain-specificity:
Essential cookies are small data files. They can be used for a range of different purposes, **such as customizing a website for a particular user, improving that user's website experience, storing some information when you move between pages, and knowing if you are logged in (save the status without saving password) and, optionally, remembering you between visits.**

Implication-oriented:
Essential cookies are small data files. They can be used for a range of different purposes. **If you visit a secured website requiring a password, essential cookies are what allow you to navigate between pages without having to log in every time. It still poses security threats to users because it collects personal data about browsing habits. Such information is vulnerable to data breaches and attackers.**

After reading the above policy snippet, which answers do you think are correct regarding "**Essential Cookies**" in relation to this Alexa Skill?
1. This Skill may collect what you look through when you use your Alexa device to view some other applications like Facebook.
2. This Skill may save your login status and may not save your password.
3. The attacker may track your browsing history if he has access to the essential cookies.
4. The attacker may know your Alexa device type if he has access to the essential cookies.

3. Policy Snippet: "*Information we may collect and share - See it for details of who we share to and why. Academic researchers: For activities such as statistical analysis and academic study, but only in a pseudonymised format.* ***Pseudonymous data*** *is where your data is identified by a code rather than your name or other information that directly identifies you.*"

Domain-specificity:
Pseudonymous data is data that has been de-identified by replacing any information which could be used to identify an individual with a pseudonym. **In this way, it does not contain explicit personal data, but only unique references to it, like only showing the same piece of an IP address (meaning users in the same network), the same wake words for most people using an Alexa device. (The wake words are to wake up the Alexa device, like "Hi, Siri" on iPhone.) Such information cannot apply to a specific person.**

Implication-oriented:
Pseudonymous data is data that has been de-identified by replacing any information which could be used to identify an individual with a pseudonym. **However, it still has re-identification risks if an attacker has enough techniques. When attackers have some other user datasets, they may infer users' data to identify a specific person with the pseudonymous data. For example, an attacker can identify 87 per cent of US citizens if they know their gender, date of birth and ZIP code.**

After reading the above policy snippet, which answers do you

think are correct regarding "**Pseudonymous data**" in relation to this Alexa Skill?
1. The shared pseudonymised data may still include some common part of your location (like the US, Australia, New York, or London) if the Skill has collected them.
2. The pseudonymised data may contain some information that can apply to a specific person.
3. The attacker may re-identify your home address if he uses enough techniques when having your pseudonymous data.
4. The attacker cannot infer your information like phone number using pseudonymous data with other stolen datasets.

4. Policy Snippet: "*How we collect and use your personal information by Ecovacs*
To maintain the quality of our services and the safety of your information, when you visit our website and use the services provided by Ecovacs, we may record types and modes of services, the operation information during your services and any other log information in connection with your services including your IP address, system version, ***IMEI and MEID of your mobile device****, and your location.*"

Domain-specificity:
IMEI stands for International Mobile Equipment Identity. It is a unique 15-digit number assigned to all cellular devices. The 14-digit MEID stands for Mobile Equipment Identifier and is similarly meant to identify a mobile device. **You may need this number to unlock your mobile phone or tablet, to track or detect a lost or stolen mobile phone, or to see if your mobile phone will work on another carrier's network.**

Implication-oriented:
IMEI stands for International Mobile Equipment Identity. It is a unique 15-digit number assigned to all cellular devices. The 14-digit MEID stands for Mobile Equipment Identifier and is similarly meant to identify a mobile device. **It can be used to block or blacklist your mobile phone. If the attacker calls the telecom provider with a report of a stolen mobile phone, then after providing the necessary details for verification and the IMEI number, the mobile phone can be blocked, resulting in it being unusable.**

After reading the above policy snippet, which answers do you think are correct regarding "**IMEI and MEID of your mobile device**" in relation to this Alexa Skill?
1. The Skill may collect information about your telecom providers based on the IMEI and MEID of your mobile device.
2. The Skill may collect your voice ID through IMEI and MEID of your mobile device.
3. The attacker may track your device's location when having the IMEI and MEID of your mobile device.
4. The attacker may access your Alexa device associated with your mobile when having the IMEI and MEID of your mobile device.

5. Policy Snippet: "*If you are a California resident, the information below also applies to you.*
Categories of personal information collected and disclosed for a business purpose: We may collect and share the personal information collected with the third-party service provider:
**Technical or internet data to detect security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity*
Internet user or* ***traffic data*"

Domain-specificity:
Traffic data is data collected about an individual's use of an electronic network. **This data could concern the routing, timing, and duration of any device information about your settings. For example, the start time when using the Skill and the schedule for using the Skill (traffic data is any data that is needed to access such functionality).**

Implication-oriented:
Traffic data is data collected about an individual's use of an electronic network. **If you set up the cleaning schedule and your traffic data is stolen, the attacker may know your schedule about using this device and any data to make such functionality. He may infer some information about you.**

This Skill will work with Amazon Alexa, giving you the ability to use voice control to start and stop cleaning your home using a vacuum, set up a cleaning schedule, and much more. After reading the above policy snippet, which answers do you think are correct regarding "**traffic data**" in relation to this Alexa Skill?
1. This Skill may collect and share the end time of using the Alexa device based on the traffic data.
2. This Skill cannot collect and share the WIFI data of the Alexa device based on the traffic data.
3. The attacker may infer your daily clean routine if he has your traffic data.
4. The attacker may infer your home address if he has your traffic data.

6. Policy Snippet: "*Sirius XM may use HTML5 or "****Media Stamp****" technology provided by Ringleader Digital, a form of information collection that is locally stored on your device and does not rely on traditional browser cookies. HTML5 is used as a substitute for traditional cookies that often do not function well on mobile devices and may follow a user across websites. Please see your device's browser's help function or support area about your choices to clear such locally stored cookies.*"

Domain-specificity:
Media Stamp, a device identification technology, is provided by Ringleader Digital company. **A 'stamp' is used by a mobile advertising company to track internet users even when they delete cookies. By "stamping" a mobile device, the Skill can identify the visitors and track their clicks, impressions and acquisitions across all browsing sessions, mobile sites and wireless carriers. Additionally, Media Stamp can enable advertisers to provide targeted, relevant advertisements to the users.**

Implication-oriented:
Media Stamp, a device identification technology, is provided by Ringleader Digital company. **It can use a 'stamp' to represent you and track your online behavior, like your browsing history. However, it may allow Skill to track users' online activity without their consent. The Media Stamp allows Ringleader Digital, advertisers, ad agencies and website publishers to track your web browsing movements across the entire internet and not just one particular website. It means that anyone (Skill or other third parties) with your 'stamp' can track your online behavior.**

After reading the above policy snippet, which answers do you think are correct regarding "**Media Stamp**" in relation to this Alexa Skill?
1. The Skill may collect you're the time that you use the Skill if it uses the Media Stamp.
2. The Skill may collect information about what advertisements you clicked on if it uses the Media Stamp.
3. The attacker may infer your IP address if he knows the Media Stamp.
4. The attacker cannot track your phone number if he knows the Media Stamp.

7. Policy Snippet: "*This Site does not knowingly collect, use, or disclose Personal Information from children under the age of 13 without prior parental consent, except as permitted by COPPA.*
We may collect Other Information automatically from your child's computer or device, such as the frequency with which the child visits our Site and the pages visited, to support the internal operations of the Site. We collect this information so we can understand and monitor usage of the Site, customize content on the Site and improve the performance of the Site. This information is collected using technologies such as cookies, ***web beacons****, and similar technologies. This information is not used to behaviourally target children and we do not permit behavioural targeting on any of our Services that are directed to children.*"

Domain-specificity:
A web beacon is a technique used on web pages and emails to (usually invisibly) allow checking that a user has accessed some content. **Web beacons are typically used by third parties to monitor the activity of users at a website for the purpose of analytics services. It can help the experience for users. It can be used when monitoring online ad impressions, understanding user behaviour, and tracking the success of ad campaigns.**

Implication-oriented:
A web beacon is a technique used on web pages and emails to (usually invisibly) allow checking that a user has accessed some content. **However, the attacker can use such web beacons to analyse the information about the location of individuals. Additionally, some third parties will use web beacons to send users personalized advertising through email. The attacker also has to change to use such email.**

After reading the above policy snippet, which answers do you think are correct regarding "**web beacons**" in relation to this Alexa Skill?
1. The Skill may collect your online browsing information based on your web beacons.
2. The Skill may use web beacons to get your online contact information.
3. The attacker may know your Alexa device type if your web beacons are stolen.
4. The attacker may send you lots of phishing emails if your web beacons are stolen.

8. Policy Snippet: "*What and How long Doppio keeps your personal data? Live recordings and transcripts of what you say while playing in one of our Zoom Apps. Transcripts are stored for one year and then purged. Fully* ***anonymized audio recordings*** *may be retained indefinitely.*"

Domain-specificity:
Anonymized audio recordings mean that such recordings cannot be tracked back to you or used to identify you. **Anonymous means that data is collected or de-identified in such a way that the identity of any subject cannot be discerned through the data. For example, such anonymized audio recordings cannot be used for voice recognition. But it still contains the information that you said.**

Implication-oriented:
Anonymized audio recordings mean that such recordings cannot be tracked back to you or identified you. **When the device setting or processing environment is identified, "anonymized" can be threatened or compromised even when direct identifiers have been removed from the data.**

After reading the above policy snippet, which answers do you think are correct regarding "**anonymized audio recordings**" in relation to this Alexa Skill?
1. This Skill cannot collect your home address with the anonymized audio recordings if you ever said it to the Alexa device.
2. The Skill cannot use anonymized audio recordings to identify your voice ID to wake and use the Alexa device.
3. The attacker may get personal information about you from the anonymized audio recordings if you ever said such information to the Alexa device.
4. The attacker may create a fake voice about you by using anonymized audio recordings.

9. Policy Snippet: "*We inform you herein about how we collect your Personal Data and to what purposes we process your Personal Data. If You Subscribe to Newsletters and Other Marketing Communications: In order to send you our newsletter, we use "Klaviyo," a service provided by newsletter platform Klaviyo Inc., Boston, Massachusetts, USA. The data you provide us with in order to receive the newsletter will be transferred to a server provided by Klaviyo Inc. located in the USA and stored there. For this purpose, we have agreed to the* ***Standard Contractual Clauses****. Klaviyo will use this information in order to send the newsletter on our behalf, but according to information available from Klaviyo, can also use this data in order to optimize or improve its own services, e.g., for technical optimization of the sending process*

as well as presentation of the newsletter or for economic reasons, and to determine from which countries subscribers come. Nevertheless, Klaviyo represents it will not use your data to forward them to third parties or to contact you directly."

Domain-specificity:
Standard Contractual Clauses are standard sets of contractual terms and conditions which both the sender and the receiver of the personal data sign up to. **It ensures appropriate data protection safeguards and can be used as a ground for data transfers from the EU to third countries. Alexa Skill needs to guarantee your data security when transferring your data.**

Implication-oriented:
Standard Contractual Clauses are standard sets of contractual terms and conditions which both the sender and the receiver of the personal data sign up to. **If the Alexa Skill does follow such clauses, they will protect your data when transferring your data from the EU to third countries. Otherwise, the attacker will get all the collected information by the Alexa Skill.**

After reading the above policy snippet, which answers do you think are correct for the "**Standard Contractual Clauses**" about this Alexa Skill?
1. These Clauses are intended to guarantee that the Alexa Skill needs to protect your data when transferring among any countries.
2. These Clauses may be applied when transferring data between the EU and other countries.
3. If the Skill follows these Clauses, the attacker can obtain your email address with 100% success when transferring data.
4. If the Skill follows these Clauses, the attacker may not obtain your location when using Klaviyo.

10. (Attention Check question)
Only for control group:
*The Alexa Skill needs to provide a **privacy policy** for users. The privacy policy should include some information like: 1) what data the Skill will collect from users; 2) what data the Skill will use; 3) what data the Skill will share with others; 3) what data the Skill will retain; 4) what data the Skill will protect and how the Skill will protect; 5) what rights that users have; etc. It doesn't contain users' comments about the Skill. The privacy policy is not only to protect users' rights and data, but also to protect Skill's legal rights. If the Alexa Skill doesn't follow its provided privacy policy, it will violate some data protection regulations.*

Only for two experimental groups:
*The Alexa Skill needs to provide a **privacy policy** for users. The privacy policy is not only to protect users' rights and data, but also to protect Skill's legal rights. If the Alexa Skill doesn't follow its provided privacy policy, it will violate some data protection regulations.*
Explanation sentences: The privacy policy should include some information like: 1) what data the Skill will collect from users; 2) what data the Skill will use; 3) what data the Skill will share with others; 3) what data the Skill will retain; 4) what data the Skill will protect and how the Skill will protect; 5) what rights that users have; etc. It doesn't contain users' comments about the Skill.

After reading the above sentences, which answers do you think are correct for the "**privacy policy**" about this Alexa Skill?
1. The privacy policy is intended to protect Skill's legal rights.
2. The privacy policy contains users' comments about the Skill.
3. The privacy policy contains descriptions about what data Skill will collect from users.
4. The Skill does not need to provide a privacy policy for users.

11. Policy snippet: "*Your ecobee Device will collect environmental data such as temperature and humidity as well as operational data such as temperature set points from your HVAC equipment. Some Device models may include additional types of data such motion sensing (i.e., "occupancy sensing"). Depending on your Device model, your Device may also collect data from remote sensors in addition to the Device itself. Using machine learning with both on-device and remote processing, environmental, operational HVAC and occupancy sensing data and is used to **optimize the heating and cooling algorithms** on your Device to minimize energy usage when you are home or away. Collectively, this is known as Device Data. For ecobee Smart Security users, occupancy-sensing data can be used to arm or disarm your home monitoring solution.*"

Domain-specificity:
The heating and cooling algorithms are part of the Alexa Skill's functionality. The Skill will use the collected information to optimize the algorithms better for your own home. **This can be used to improve your experience. For example, when the room temperature is proper, the Skill can stop the heating and cooling algorithms to save electricity.**

Implication-oriented:
The heating and cooling algorithms are part of the Alexa Skill's functionality. The Skill will use the collected information to optimize the algorithms better for your own home. **The risk for heating and cooling algorithms is very low. The attacker is hard to modify the designed algorithms and is also difficult to get some information from such optimized algorithms.**

This Skill is called ecobee. You've always been able to ask Alexa to control your ecobee device(s). Now you can ask it to control your ecobee home monitoring solution and your ecobee cameras. After reading the above policy snippet, which answers do you think are correct regarding the phrase "**optimize the heating and cooling algorithms**" in relation to this Alexa Skill?
1. The Skill may change the algorithm for heating or cooling based on the real situation of your home.
2. The Skill may use your home address to optimize this algorithm.
3. The attacker may control the Alexa device when knowing the heating and cooling algorithms.
4. This algorithm may be useless for an attacker to steal your personal information.

12. Policy Snippet: "*SPE (Sony Pictures Entertainment) may use information about you, including **SPE-Collected PI** and other Personal Information, for any purposes consistent with SPE's statements under this Privacy Policy and not prohibited by applicable law. SPE may*

*also share any information about you (including, without limitation, **SPE-Collected PI**) for any purposes consistent with this Privacy Policy, or otherwise not prohibited by applicable law.*"

Domain-specificity:
Personal information, also called "PI", is information that can identify an individual. **It may contain direct identifiers (e.g., passport information, audio recording when using the Alexa devices) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.**

Implication-oriented:
Personal information, also called "PI", is information that can identify an individual. **It can be sensitive or non-sensitive. Sensitive PI includes legal statistics, like credit card information and passport information. With a few bits of PI, the attacker can create false accounts in the person's name. Companies normally use some techniques to obscure the PI, so it is received in a non-personally identifiable form. Non-sensitive PI is easily accessible from public sources like phonebooks, the Internet, and corporate directories. This type of information cannot be used alone to determine an individual's identity.**

After reading the above policy snippet, which answers do you think are correct for the term "**SPE-Collected PI**" in relation to this Alexa Skill?
1. This Skill may collect your phone number.
2. This Skill may collect your Alexa device version.
3. The attacker may send you lots of phishing emails if your SPE-Collected PI is stolen.
4. The attacker may get your account password if your SPE-Collected PI is stolen.

13. Policy Snippet: "*We use Google AdSense Advertising on our website.*
*Google, as a third-party vendor, uses cookies to serve ads on our site. Google's use of the **DART cookie** enables it to serve ads to our users based on previous visits to our site and other sites on the Internet. Users may opt-out of the use of the **DART cookie** by visiting the Google Ad and Content Network privacy policy.*"

Domain-specificity:
The DART cookie helps marketers understand how well their Internet advertising campaigns or paid search listings perform. **When a user lands on a website showing Google ads, the DART cookie is dropped on the user's browser. It gathers data to enable AdSense publishers to serve ads on their blogs and websites and to improve advertising. DART cookie helps provide marketers some information, like the number of users their advertisements were displayed to, how many users clicked on their Internet ads or paid listings, and which ads or paid listings they clicked on. It does not collect any personal information.**

Implication-oriented:
The DART cookie helps marketers learn how well their Internet advertising campaigns or paid search listings perform. **It aims to collect and track your online advertisement browsing behavior. All advertising publishers are required to notify users if their website is using DART cookies and must clearly display the notification within their privacy policy. Users can opt-out of the DART cookie (delete the DART cookie). It will not collect users' personal information. So the attacker cannot use the DART cookie to identify you or track back to you.**

After reading the above policy snippet, which answers do you think are correct regarding "**DART cookie**" in relation to this Alexa Skill?
1. The Skill may collect your contact information if it uses the DART cookie.
2. The Skill may collect information about which advertisement you clicked if it uses the DART cookie.
3. The attacker may not know your home address if your DART cookie is stolen.
4. The attacker may know the advertisements you browsed if your DART cookie is stolen.

14. Policy Snippet: "*Third Party Tracking and Online Advertising: We may share information about your use of our Services over time, including location information, with third party ad networks, social media companies and other third parties so that they may play or display ads that may be relevant to your interests on our Service as well as on other websites, apps or services, or on other devices or advertising channels. You may, of course, decline to submit any personal information through the Service, in which case Life360 may not be able to provide its Services to you.*
*Cross-device linking. Please note that opting-out of receiving interest-based advertising through the NAI's and **DAA's online resources** will only opt-out a user from receiving interest-based ads on that specific browser or device, but the user may still receive interest-based ads on his or her other devices. You must perform the opt-out on each browser or device you use.*"

Domain-specificity:
The Digital Advertising Alliance (DAA) is an association that is mainly known for running and enforcing the Online Behavioural Advertising self-regulatory program AdChoices. **It establishes and enforces responsible privacy practices across the industry for relevant digital advertising, providing users with enhanced transparency and control for online advertisements. Users can opt-out of receiving advertising and sharing information under DAA's resources and practices.**

Implication-oriented:
The Digital Advertising Alliance (DAA) is an association that is mainly known for running and enforcing the Online Behavioural Advertising self-regulatory program AdChoices. **It provides a privacy policy for relevant digital advertising, gives consumers information and control over the types of digital advertising they receive. The attacker is hard to control such advertising from DAA's resources. Those interest-based advertisements are only designed and posted for users' experience.**

After reading the above policy snippet, which answers do you think are correct regarding "**DAA's online resources**" in relation to this Alexa Skill?
1. The Skill may share the collected information with third parties under DAA's resources.
2. Users cannot opt-out of sharing the collected information with third parties under DAA's resources.
3. The attacker can access to your Alexa device using the sent advertisements from DAA's online resources.
4. The attacker may infer your interests if they are able to send you sufficient advertisements.

15. Policy Snippet: "*Life360 does not knowingly collect personal information from children under the age of 13 (a "child") without verifiable consent of a parent or guardian and the Service is intended to be used by children under 13 only with significant parental involvement and approval.*
We collect and share information about a user's device (e.g., IP address, device type/model/manufacture / operating system, and a unique ID that allows us to identify the browser, mobile device or account, such as a UDID, ***IDFA****, Google AdID or similar) as well as certain usage information about the use of the Service (for example, whether the user opens emails) and we collect analytics data. We collect geolocation data through the device IP address, WiFi, Bluetooth and GPS coordinates available through the user's mobile device and through technologies and sensors that may be nearby.*"

Domain-specificity:
The Identifier for Advertisers (IDFA) is a special identifier, assigned by Apple to a user's device. **It allows an installed mobile application to track user behaviour across other companies' apps, and websites. It is not the IP address. Such information can be used for the purposes of advertisement targeting and personalization. IDFA enables advertisers to track a user's interactions within mobile apps, such as downloads, clicks and purchases.**

Implication-oriented:
The Identifier for Advertisers (IDFA) is a special identifier, assigned by Apple to a user's device. **Some developers can use IDFA to collect data about what people do on their phones and use that data to deliver targeted advertisements. Such developers might have a history of abusing user privacy and safety.**

After reading the above policy snippet, which answers do you think are correct regarding "**IDFA**" in relation to this Alexa Skill?
1. The Skill and advertisers may infer your interests using the shared IDFA.
2. The Skill and advertisers may collect your IP address using the shared IDFA.
3. The attacker may analyse your online behaviours if your IDFA is stolen.
4. The attacker may access to your Alexa device if your IDFA is stolen.

16. Policy Snippet: "*YOUR CHOICES ABOUT YOUR INFORMATION Close Your Account or Delete Personal Information: We retain your information for as long as your account is active or as reasonably necessary to maintain the Service, meet legal and accounting obligations, and for the other purposes described in this Privacy Policy. If you wish to close your account, and/or request to delete your personal information, please contact us at privacy@life360.com. When account information is deleted or de-identified, certain residual information may remain within our* ***archive records****, such as for customer and technical support, billing and tax purposes.*"

Domain-specificity:
Archive records are a kind of backup record. **When users delete their personal information in Skill, it may still retain some information for specific purposes. Such information may include your personal information. For technical support purposes, the Skill may retain your technical reports, like the Skill bugs reports. For billing and tax purposes, Skill may retain your payment history.**

Implication-oriented:
Archive records are a kind of backup records. **After deleting your information, the Skill may retain some specific information about you for their purposes. Such information is stored as archive records and may include some personal information. For billing and tax purposes, Skill may retain your payment history, including your payment account information. If attackers obtain such kind of archive records, they may know some detailed information about you.**

After reading the above policy snippet, which answers do you think are correct regarding "**archive records**" in relation to this Alexa Skill?
1. For customer support purposes, Skill may retain your order history about its services.
2. For billing and tax purposes, the Skill may retain your voice ID.
3. If the Skill retains some information about you for billing and tax purposes, the attacker may learn your home address when the archive records are stolen.
4. If the Skill retains some information about you for technical support purposes, the attacker may know your date of birth when the archive records are stolen.

17. Policy Snippet: "*Under certain circumstances, you have rights under data protection laws in relation to your personal data.* ***Request erasure of your personal data****. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.*"

Domain-specificity:
Request erasure of your personal data. The data protection regulation gives individuals the right to ask organizations to delete their personal data. **You can request to delete the collected personal**

data if 1) You withdraw your consent; 2) The Skill process the personal data through unlawful means, etc. If Skill doesn't delete your personal data with unreasonable things, they will violate the data protection regulation. And users can make complaints about the Skill.

Implication-oriented:
Request erasure of your personal data. The data protection regulation gives individuals the right to ask organizations to delete their personal data. **The Skill may process or use your personal data with unlawful means. If users delete their personal data timely or remove all personal identifiers, it will reduce the risk of indirect identifiers being used to connect any stored data to a particular user.**

After reading the above policy snippet, which answers do you think are correct regarding "**Request erasure of your personal data**" in relation to this Alexa Skill?
1. You have the right to ask Skill to delete your voice recordings.
2. The Skill may not remove your email address from their datasets if they need the email address to complete the fundamental function of the Skill.
3. If you use this right, the Skill can still retain all your data whatever they need or not.
4. If you use this right to delete your information, the attacker can still get your information after attacking the Alexa Skill.

18. Policy Snippet: "*USERS' RIGHTS IN RESPECT OF THEIR PERSONAL INFORMATION*
*If you wish to exercise one of these rights, please submit your request through the **GDPR Rights** for EU Users section of your in-App Privacy Settings and click on the option to "Request my Data," "Delete my Data," or "Reset Your Data Sharing Settings," respectively.*"

Domain-specificity:
The GDPR rights are some lawful users' rights under general data protection regulation (a legal framework). **It includes: the right to be informed, the right to modification, the right to rectification, the right to restrict processing, the right to object, and also rights around automated decision-making and profiling, etc. The users have the related lawful rights to control the collected information by Skill.**

Implication-oriented:
The GDPR rights are some lawful users' rights under general data protection regulation (a legal framework). **It includes: the right to be informed, the right to erasure, the right to rectification, etc. If users don't understand such rights, the risk of their privacy being used increases. The Skill may collect, use, share or retain their data with unlawful means. With GDPR rights, users can protect and restrict the Skill to process their data.**

After reading the above policy snippet, which answers do you think are correct regarding "**GDPR Rights**" in relation to this Alexa Skill?
1. You have the right to access the collected data by the Skill under GDPR protection.
2. When you want to delete useless voice recordings, you have the right to enforce the Skill to delete them.
3. If you don't use such rights, the Skill may still retain your personal data after you uninstall the Skill.
4. Under GDPR protection, users may not protect their privacy or control their shared personal information when using the Skill.

19. Policy Snippet: "*Most web browsers and some mobile operating systems and mobile applications include a **Do-Not-Track ("DNT") setting** you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Policy.*"

Domain-specificity:
Do Not Track is a technology that enables users to opt-out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. **This lets websites know that you don't want them to track you. You don't wish for tracking from analytics or advertising networks, and you don't want information about your browsing transmitted to social networks.**

Implication-oriented:
Do Not Track is a technology that enables users to opt-out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. **If you turn on the do not track setting, Skill and its third parties will not track your online behaviour and will not obtain the contents between your social networks. It will reduce the risk of analysing your online activities.**

After reading the above policy snippet, which answers do you think are correct regarding "**do not track setting**" in relation to this Alexa Skill?
1. The Skill may analyse your online usage behaviour if you turn on the "do not track" setting.
2. The Skill may allow third-party advertising services to identify you without your consent if you turn on the "do not track" setting.
3. The Skill cannot analyse your browsing interests if you turn on the "do not track" setting.
4. If you turn off the "do not track" setting, the attacker may track your browsing history when hacking the Alexa Skill.

20. Policy Snippet: "*YOUR DATA PROTECTION RIGHTS (EEA VISITORS ONLY)*
If you are a resident of the EEA, subject to applicable law, you may have certain rights regarding your personal information. Specifically, you may be able to make the following choices:
*Object to processing of your personal information, ask us to restrict processing of your personal information or **request portability of***

your personal information *by contacting us using the contact details provided under the "Contact Us" heading below."*

Domain-specificity:
The right to data portability gives users the right to receive personal information they have provided to the Skill. **It also gives users the right to request that the Skill transmits their personal information directly to others (another Skill, website or application). If you use Skill to browse Facebook, you can request the Skill transmit some information (like your account information or your contact information) directly to Facebook. Thus, Facebook may be able to suggest your friends' accounts to you.**

Implication-oriented:
It means that users have the right to receive the personal information that they have provided to the Skill and **also have the right to transmit the personal information to others (another Skill, website or application). You can ask Skill directly to transmit your personal information to others. Or you can transmit your personal information (received from the Skill) to others by yourselves. However, it means the security of the user's personal information is your responsibility until it safely reaches its destination (another Skill, website or application). It is important not to lose track of information while it's being transferred.**

After reading the above policy snippet, which answers do you think are correct regarding "**request portability of your personal information**" in relation to this Alexa Skill?
1. Users may request the Skill to link their personal information with other Skills.
2. Users cannot transmit their contact information to other Skills by themselves.
3. Users may protect their personal information by themselves if they request the portability of their personal information.
4. The attacker may obtain users' personal information if users transmit their personal information to a fake or illegal application or Skill.

21. (Attention Check question)
Only for control group:
*Our **survey** examines users' understanding of the Alexa Skill's privacy policy and relevant technical terms. You have rights to withdraw your participation. If you want to withdraw, you can just close the page. Your answer will not be saved and we will not collect your answer after you withdraw. But please note that: You must complete all questions seriously. Otherwise, you won't be paid. The terms that we examine are hard or common terms in the privacy policy. You may know or understand these terms after completing this survey. We would like to improve your privacy awareness by answering this survey.*

Only for two experimental groups:
*Our **survey** examines users' understanding of the Alexa Skill's privacy policy and relevant technical terms. The terms that we examine are hard or common terms in the privacy policy. You may know or understand these terms after completing this **survey**. We would like to improve your privacy awareness by answering this **survey**.*
Explanation sentences: You have rights to withdraw your participation. If you want to withdraw, you can just close the page. Your answer will not be saved and we will not collect your answer after you withdraw. But please note that: You must complete all questions seriously. Otherwise, you won't be paid.

After reading the above sentences, which answers do you think are correct for this survey?
1. This survey examines users' understanding of mental health.
2. This survey examines users' understanding of the Alexa Skill privacy policies.
3. Users have rights to withdraw from this survey.
4. We will still save your completed answers after you withdraw the survey.

22. Policy Snippet: "*(ecobee Privacy Policy) The collected information will be shared with our online shopping cart provider and payment processor. We use shopping cart features that safeguard this information by using industry standard SSL (**Secure Sockets Layer**) encrypted servers. SSL encodes the information transferred between you and the server, rendering it unreadable to anyone trying to intercept the information. Your credit card data (which is never seen or recorded by ecobee) will be deleted by the cart provider and payment processor in 30 days.*"

Domain-specificity:
Secure Sockets Layer is the standard technology for keeping an internet connection secure. It will safeguard any sensitive data that is being sent between two systems. **It will also prevent criminals from reading and modifying any information transferred, including potential personal details. When you use the Alexa device, you may speak to it. The device may need to transfer your voice or audio data (sensitive data) via the Internet. This technology will protect the data between two systems.**

Implication-oriented:
Secure Sockets Layer is the standard technology for keeping an internet connection secure. It will safeguard any sensitive data that is being sent between two systems. **If the Alexa doesn't apply such technology, it will increase the risk of disclosing your sensitive data to attackers. The attacker can pretend a legal user or device to send and store your sensitive data.**

After reading the above policy snippet, which answers do you think are correct regarding "**Secure Sockets Layer**" in relation to this Alexa Skill?
1. Your data about the interaction with the Alexa device may be protected within the transmission.
2. If the Skill uses a related sensor, the sensor information may not be protected within the transmission.
3. With this technology, the attacker cannot obtain the information that has stored in a system.
4. The attacker may still send and get your information using a fake account.

23. Policy Snippet: "*If Life360 learns that we have **inadvertently collected personal information of a child** without parental consent, we will take appropriate steps to delete this information. If you are a parent or guardian and discover that your child under the age of 13 has a registered account with our Service without your consent, please alert us immediately by emailing privacy@life360.com so that we may delete that child's personal information from our systems.*"

Domain-specificity:
It means that the Skill may accidentally collect children's personal information even though it should not, **such as audio or voice information, and their online behavior. If this happens and Life360 becomes aware of it, the personal information will be immediately deleted from their systems, like the Skill cannot get it or recover it again.**

Implication-oriented:
It means that the Skill may accidentally collect children's personal information even though it should not. **Generally, the Skill needs to delete all child's personal information. If the data still can be recovered or the Skill doesn't have such policies, the children's privacy cannot be guaranteed and the Skill may violate some data protection regulations.**

After reading the above policy snippet, which answers do you think are correct regarding "**inadvertently collected personal information of a child**" in relation to this Alexa Skill?
1. The Skill may delete any sensitive information collected from children without their parent's consent once it becomes aware of such collection.
2. If the parent gives consent for the child to use the device, the Skill may collect children's language speech information.
3. If the Skill deleted child's personal data in their system, the attacker may not obtain it from the Skill's system.
4. The Skill can re-process the children's information after deleting it from the dataset.

24. Policy Snippet: "*This section applies to you if you are a resident of the state of California (a "consumer"). California law requires us to disclose certain information regarding the categories of personal information we collect. For purposes of this section, "personal information" has the meaning provided by the **California Consumer Privacy Act** (the "CCPA") and does not include information that is publicly available, that is deidentified or aggregated such that it is not capable of being associated with an identifiable consumer or device.*"

Domain-specificity:
The California Consumer Privacy Act (CCPA) is a law that allows any Californian consumer to demand access to the information a company has saved on them, as well as a full list of all the third parties that the information is shared with. **The type of collected and shared data is defined by this law, like defining the meaning of personal information. CCPA also defines what kind of third parties are not. It means that the Skill cannot provide the collected users' information for such parties.**

Implication-oriented:
The California Consumer Privacy Act (CCPA) is a law that allows any Californian consumer to demand access to the information a company has saved on them, as well as a full list of all the third parties that the information is shared with. **Once the Skill collects or shares some data beyond the defined range. Users can request the Skill delete such information. Users also have rights about not sharing the information with any third parties. Under CCPA, the Skill needs to identify security risks for protecting users' privacy.**

After reading the above policy snippet, which answers do you think are correct regarding "**California Consumer Privacy Act**" in relation to this Alexa Skill?
1. The Skill can share some information covered by CCPA with its connected device.
2. If the CCPA defines "A" is not the third party, the Skill can share users' data with "A".
3. The Skill can share some information without your consent, and you cannot reject it.
4. The Skill needs to try to prevent some illegal activities for your privacy.

25. Policy Snippet: "***Alexa Communication Schedule**: AMCS LLC ("AMCS"), an affiliate of Amazon, may offer you certain Alexa-related communication services, such as the ability to send and receive messages and calls and connect with other Alexa users, and the ability to place outbound calls to phone numbers (collectively, "Alexa Communication"). This schedule is part of the Alexa Terms of Use and you agree to these terms when you register for or use Alexa Communication. Your use of Alexa Communication is also subject to the Alexa Communication Usage Guidelines, which are part of this schedule. AMCS and its affiliates may offer services other than Alexa Communication, which are not covered by this schedule and may be subject to other terms.*"

Domain-specificity:
Alexa allows users to place calls and send and read SMS messages via voice using the mobile phone paired to the head unit. Alexa can also drop-in, make announcements and send voice messages to other Alexa devices, including the Alexa App. **To call or send an SMS to any contact by name, users may grant Alexa permission to upload contacts and access SMS from their mobile phone. In other words, to enable this communication, Alexa may collect related information, like your contact information, your device information, communication recordings, etc.**

Implication-oriented:
Alexa allows users to place calls and send and read SMS messages via voice using the mobile phone paired to the head unit. Alexa can also drop-in, make announcements and send voice messages to other Alexa devices, including the Alexa App. **Alexa has a related policy to describe the collection, use, sharing and security of the data. Alexa needs to protect such data. Otherwise, the attacker can obtain any information about your communication with others.**

After reading the above policy snippet, which answers do you think are correct regarding "**Alexa Communication Schedule**" in relation to this Alexa Skill?

1. The Alexa may collect your message recordings when you contact others using Alexa.

2. The Alexa may not collect your voice recordings when you contact others using Alexa.

3. The Alexa cannot share the collected data about the communications (like the message you send) to do the analytic services.

4. The Alexa may guarantee your data security if it collects some data about communications (like the message you send).