Opening statement

Good afternoon. I am the Director of Privacy for Apple in Europe, Worldwide Director of Privacy Compliance and the appointed Data Protection Officer in Europe under the GDPR.

I thank the Chair and the Members of the Committee for the opportunity to speak to you today on the important issue of voice assistants and the use of data.

Apple has been operating in Cork since 1980 and we're proud of the many contributions we make to the economy and job creation. We employ 6,000 people in Ireland. Over the last four years, we've spent more than €1 billion with local companies, and our investment and innovation supports more than 27,000 jobs up and down the country.

We believe privacy is a fundamental human right. Our approach to privacy is different from that of other tech companies. We design our products from the ground up to minimise the amount of data Apple collects and we work vigilantly to protect our customers' personal data and give them control over their information.

Privacy is an issue larger than one company or one country, which is why we strongly support the GDPR and advocate for other countries to adopt similar approaches that deliver a highly effective and necessary framework.

During the Committee's session last week, the discussion emphasised Article 25 of the GDPR, concerning privacy by design. This is a core value and fundamental principle that Apple has embodied from the beginning.

Privacy is at the heart of every product and service we create, and we continually develop innovative technologies and techniques designed to minimise how much customer data we, or anyone else, can access while delivering world class services to our customers.

Privacy by design applies to all of Apple's services. That includes Siri, Apple's intelligent assistant. Like all of our services, our goal with Siri is to create the best user experience while vigilantly protecting user privacy.

We introduced Siri in 2011 as an integral part of our products, helping users get things done faster and easier. This includes tasks like making calls, sending messages, setting alarms, getting directions, finding photos and playing music and TV shows, just to name a few.

Like other Apple services, we minimise the amount of data Siri collects and use that data only to improve Siri. We don't use Siri data to build a marketing profile, and we never sell it to anyone. Our product is the technology we create — not the customer.

We've built privacy protections into Siri according to some core principles that demonstrate our comprehensive approach to protecting user data.

First, Siri uses as little data as possible to deliver an accurate result. When you ask a question about a football match, for example, Siri uses your general location to provide suitable results. But if you ask for the nearest supermarket, more specific location data is used.

Second, we design Siri to operate with the most sensitive data on device instead of having to send everything through Apple servers. For example, if you ask Siri to read your unread messages, the content of your message never leaves your device and is not transmitted to Siri's servers because that isn't necessary to fulfill your request. This means that messages are not available to Apple or any other third party.

Third, requests made to Siri are not linked to your Apple ID, phone number or email address. Instead, they are associated with a random identifier — a long string of letters and numbers associated with a single device to keep track of data while it's being processed. This is a feature we believe is unique among the digital assistants in use today.

As the Committee heard last week, to improve voice assistants such as Siri, there is a need for human review of a very small sample of audio interactions.

This helps to ensure that Siri understands users' questions and provides the right answer. For example, Siri has to recognise my Irish accent and all of yours, and you can understand the complexity if you multiply that across the different languages, dialects, and styles of speech in the countries where we do business.

However, I want to be clear that human review of audio samples has always been conducted on a very small subset of audio samples from Siri requests. And the people reviewing the audio samples are not shown an Apple ID, phone number, or email. As I mentioned earlier, all Siri requests are associated with a random identifier.

This August, customer concerns arose in regard to human review of Siri audio samples. In response, we immediately suspended human review of Siri audio requests, reviewed our practices and policies, and released the following improvements to Siri's privacy protections:

— **First**, by default, we no longer retain audio recordings of Siri interactions.

— **Second**, users now have the choice to help Siri improve by learning from audio samples of their requests. For users who choose to share their audio it is still only associated with the random identifier that I mentioned earlier.

— **Third**, if customers do choose to help improve Siri, only Apple employees — not contractors — will be allowed to listen to audio samples of Siri interactions for the limited review purposes I described earlier. Additionally, our team will work to delete any recording which is determined to be the result of an inadvertent trigger of Siri.

— **And finally**, there is now a "Delete Siri and Dictation History" option in Settings that makes it easy for users to delete Siri requests that have been retained for six months or less.

Our mission is to make products and services that enrich the lives of our customers. Unlike others, we don't view our customers and their data as the product. That is why we build privacy protections into everything we do. It is why we intentionally limit our own access to customer data.

Our products and features include innovative privacy technologies and techniques designed to minimise how much of your data we — or anyone else — can access. We believe that users should control their data and they should understand how their data is used, stored and protected.

That's the approach we bring to Siri and all the services we offer. You don't sign in with your Apple ID to use Siri, and your device processes

as much information as possible without sending it to Apple’s servers. And powerful security features help prevent anyone except you from being able to access your information. We are constantly working on new ways to keep your personal information safe.

We look forward to continuing our partnership to build on the GDPR's progress and strive for the highest standard of user privacy protection. I look forward to answering your questions.

Thank you.