Joint Committee on Communications, Climate Action and Environment
Facebook, Opening Statement
April 17, 2018

I'd like to thank the Committee for asking us to be here today to talk about the events that have come to light in recent weeks and the steps we are taking to address them.

My name is Joel Kaplan, and I'm the Vice President for Global Policy at Facebook. I'm joined here today by Niamh Sweeney, our Head of Public Policy for Facebook Ireland.

Niamh and I are also accompanied by Richard Allan, a Vice President for Policy in EMEA, Gareth Lambe, Vice President and Head of Facebook Ireland, Eva Nagle, Regulatory Counsel, and Claire Rush, Content Counsel. Niamh, Gareth, Eva and Claire are all based here in our International Headquarters in Dublin.

I want to start by echoing our CEO, Mark Zuckerberg: what happened with Cambridge Analytica represents a huge violation of trust, and we are deeply sorry.

I understand your concerns - they are shared by many people around the world - and welcome the fact that you are willing to engage with us on this topic.

We now serve more than 2 billion people around the world who use our services to stay connected with the people that matter to them most.

We know we have a responsibility to the Facebook community, and that people will only feel comfortable using our service if their data is safe.

As our second largest office globally, Facebook Ireland plays an important part in providing that service, with over 2,500 people working across multiple teams at our International HQ in Dublin's docklands.

As our CEO explained last week, Facebook is an idealistic and optimistic company. For most of our 14-year existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they care about, make their voices heard, and build communities and businesses.

But it’s clear now that we didn’t do enough to prevent these tools from being used for harm as well. We didn’t take a broad enough view of our responsibility, and that was a mistake.

It’s not enough to give people control of their information, we have to make sure that developers who get users’ consent to access data are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good.

It will take some time to work through all of the changes we need to make, but we are committed to making them, and to getting it right.

<u>What Happened</u>

In 2007, we launched Facebook Platform - meaning, the architecture of how users share information with apps (such as games) on Facebook. This is an element of the overall Facebook service people engage with every day. This was done with the vision that more apps could be social. For example, if you installed a music app, you could share playlists with your friends, and so on. To do this, we enabled people to log into apps and share who their friends were and some information about them with that app.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people globally, who agreed to share some of their Facebook information as well as some information from their friends, if the privacy settings of their friends allowed for this data to be shared.

Here is how it worked:

First, you had to be a friend of someone who installed Kogan's app. Then, if you were a friend, the app could have accessed some of your data if your permissions allowed it.

This meant that Kogan was able to access some basic profile information of up to 87 million of the friends of users that installed the app. This may have included their public profile, pages they had liked, their birthday and their current city.

Informed by the recommendations made by the DPC in their audits of Facebook, in 2014 we announced that we were changing Platform to significantly limit the information apps could access. Most importantly, apps like Kogan's could no longer ask for information about a person's friends unless their friends had also installed the app. We also required developers to get approval from Facebook before they could request any data beyond a user's public profile, friend list, and email address. These changes would prevent any app like Kogan's from being able to access as much Facebook data today.

In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is – and was – against our policies for developers to share data without people's consent, so we banned Kogan's app from our platform, and demanded that Kogan and other entities he gave the data to, including Cambridge Analytica, confirm that they had deleted all improperly acquired data — which they did.

Last month, we learned from the media that Cambridge Analytica may not have deleted the data as they had certified. We banned them – and their parent company, SCL – from using any of our services.

Cambridge Analytica continues to claim it deleted the data and has agreed to a forensic audit by a firm we hired to investigate this. We are also working with the U.K. Information Commissioner's Office – as Cambridge Analytica is established as a data controller in their jurisdiction – as it completes its investigation into what happened.

Most of the people impacted by this were predominantly in the United States – 97.1% of users who installed the app are understood to have been primarily in the US, while 81.2% of total affected people, i.e. the people who installed the app and their friends, were in the US.

However, we understand that 15 people in Ireland installed Kogan's app, and up to 44,687 people in Ireland may have been friends with someone who installed the app, and, therefore, may have been affected. This represents 0.052% of the total number of people affected, but any number is too many.

What We Are Doing

We have a responsibility to make sure what happened with Kogan and Cambridge Analytica doesn't happen again. Here are some of the steps we're taking:

Safeguarding our platform. We need to make sure that developers like Kogan who got access to a lot of information in the past, can't get access to as much information going forward.

We made some big changes to Facebook Platform in 2014 to restrict the amount of data that developers can access and to proactively review the apps on our platform. This means that, today, a developer can't do what Kogan did four years ago.

But there's more we can do to limit the information developers can access using Facebook login and we are putting additional safeguards in place to prevent abuse. We have recently announced that

- We're removing developers' ability to access your data if you haven't used their app for three months.
- We're minimising the data you give an app when you approve it to only: your name, profile photo, and email address.
- We're requiring developers to not only get approval from us but also to sign a contract that imposes strict requirements in order to ask anyone for access to their posts or other private data.
- We're restricting more APIs like groups and events. An API is a software intermediary that allows two applications to talk to each other. These changes limit the type of information that can be shared from Facebook with other applications.

Investigating other apps. We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected.

Building better controls and encouraging people to manage the apps they use. We're making it easier to understand which apps you've allowed to access your data. Last week we started showing everyone a link so that you can see the apps you've used and an easy way to revoke their permissions to your data. You can already do this in your privacy settings, but we're going to put it at the top of News Feed to make sure everyone sees it.

Reward people who find vulnerabilities. We have expanded Facebook's 'bug bounty' program so that people can also report to us if they find misuses of data by app developers.

Beyond the steps we had already taken in 2014, we believe these are the next steps we must take to continue to secure our platform.

We are also notifying the 87 million users that could have been affected by Kogan's app, either because they had installed the app or because one of their Facebook friends had.

We know there's a lot of work to do here, and that this is just the beginning. In the coming weeks and months, we're planning to continue our own review as well as conversations with experts outside the company, so we can continue to do the work needed to address these issues.

We would welcome your feedback on the steps we've announced so far and any thoughts on what more we should be doing.

Facebook in Ireland

Facebook set up its first office in Ireland in 2008. We are now located across four locations in Dublin, Meath and Cork. Since 2010, we have been regulated by the Irish Data Protection Commission, subject to both Irish and EU data protection law.

Over the past four weeks we have been cooperating with the Commissioner and her office as they have sought to establish what happened, as our lead regulator, and how Irish and EU users may have been affected by Cambridge Analytica. We have shared detailed information with them about our past and current practices and we continue to engage with them on this.

I want to speak frankly: the Data Protection Commissioner has been critical of us in recent weeks. We recognise and understand those criticisms - we could have done better in responding to concerns, and we are committed to doing better going forward.

Under the General Data Protection Regulation, which takes effect on the 25th of May 2018, Commissioner Dixon and her team will become our Lead Supervisory Authority, in line with Chapter 6 of the GDPR.

Transparency is a fundamental requirement of the GDPR and our teams have been working hard for the past 18 months to make key changes to our products that will give our users greater control over their data and visibility as to how they can exercise that control. We take the GPDR very seriously – it places additional standards on companies, and that's a good thing. We need to rebuild trust with our users and complying with the GDPR is critical to that. We have been working with the DPC on our final products, and we welcome the time invested by that Office in ongoing engagement with Facebook, and the feedback we have received on our GDPR implementation plan. And we'll be happy to talk more about the changes we have announced so far.

<u>Online Advertising and Social Media (Transparency) Bill 2017</u>

I understand we will also discuss the Online Advertising and Social Media (Transparency) Bill 2017 over the course of our conversation today.

Deputy Lawless, I know that you met with Niamh and Claire back in December when you first proposed this Bill. We very much appreciate that you looked to engage with us on this from the outset. As we said to you at the time, we fully understand what your Bill is trying to achieve and

are aligned with its goals. It mirrors, in large part, what we are trying to achieve with the new ads transparency tools we have announced. We agree that, when it comes to advertising on Facebook, people should be able to see all the ads that a page is running – and when it comes to political ads, all advertisers should be verified and any ads that they run should be clearly labeled to show who paid for them.

We are working hard to build out these transparency tools and to roll them out globally, but it takes time to do that and, most importantly, to get them right. We have been testing the first of these products in Canada and hope to be able to roll it out globally this summer.

I am sure you will have comments and questions about all of these issues, so I will stop there and just say thank you again for inviting us to be here.