SECOND SET OF RESPONSES

1. Your algorithms seem incomprehensible. Don't you think that algorithms should be made public by law?

We understand that algorithms play a big role in people's lives, and that increasing transparency and control around how they work is important to European citizens.

We recognise there is a significant interest in our News Feed algorithm in particular and have been making efforts to provide further transparency about how News Feed works. We publish a lot of information through regular updates to our News Feed FYI blog. In the January 2018 blog post, for example, we explained that we are in the process of updating News Feed to prioritise posts that are more likely to spark conversations and meaningful interactions between people.

We have defined a set of core values for how we develop the News Feed algorithm and made these public here. We also explain how people can exercise control over their own personal News Feed in our Help Centre. These articles explain how you can prioritise content from specific friends or Pages you follow, how you can add or remove sources in your News Feed, and how you can view stories in a chronological order rather than sorted by the algorithm.

We continue to develop our transparency work around algorithms and are actively engaging with policymakers and academic experts to work on what more we should do. We share the objectives of helping people understand how algorithms work, ensuring that they are fair, and improving the accountability of those who manage algorithms. But we believe these objectives are more likely to be met through other processes than through pursuing a formal requirement to make algorithms public. A full publication requirement would raise challenging questions around legitimate trade secrets and threats from people who seek to manipulate systems inappropriately. We would recommend instead a process of engagement between organisations that manage important algorithms and interested parties such as policy makers and technical experts. Facebook would be an active and willing partner in such a process.

2. Europe and America have different norms on what type of content is acceptable for publication. Many Member States have called on platforms to voluntarily remove such harmful content. Do we need to create a clear set of rules defining what is or what is not allowed on platforms in Europe?

Legal regimes differ greatly around the world with some countries criminalising a wide range of speech while others have much more permissive regimes. Most internet services that allow users to share content do not simply apply the legal standard of any particular country but have also developed their own standards for what is and is not allowed and apply these globally.

These standards are aimed at ensuring the service meets the expectations of users which will vary from service to service. For example, services directed to adult only audiences may

permit mature content while those aimed at younger users may be very restrictive and prohibit vulgar language.

Facebook has developed a set of global Community Standards aimed at meeting the expectations of our diverse community around the world. Our detailed Community Standards are published here. We believe that these standards work well for our community in Europe. We continually develop and refine them in response to feedback from users, regulators and experts. We would be happy to share more information with the European Parliament about our process for developing and applying the Community Standards if this would be helpful.

On May 15, we released numbers in a Community Standards Enforcement Report for the first time ever so that you can judge our performance for yourself. This report covers our enforcement efforts between October 2017 and March 2018, and it covers six areas: graphic violence, adult nudity and sexual activity, terrorist propaganda, hate speech, spam, and fake accounts. The numbers show you:

- How much content people saw that violates our standards;
- How much content we removed; and
- How much content we detected proactively using our technology — before people who use Facebook reported it.

We are publishing this information as we believe that increased transparency tends to lead to increased accountability and responsibility over time, and publishing this information will push us to improve more quickly too.

We do not believe that it would be appropriate to define a single set of detailed rules that would apply to all platforms given the variety of services they offer. But we do believe there is scope for a common approach in some defined areas. For example, we have found the experience of working with the European Commission in relation to hate speech and terrorist content to be a very positive one for our service and for the industry more broadly. We believe that sharing experience and agreeing on common approaches to challenging areas like these can be very beneficial.

3. Is arbitrary censorship on Facebook compatible with fundamental values of our democracy? How do you justify closing down FB pages expressing legitimate views? Does the fight against fake news justify restrictions on freedom of expression?

As explained above, Facebook has well-established Community Standards which define the boundaries of acceptable behaviour on the service. These Standards are carefully drafted and developed over time as we endeavour to ensure that Facebook remains a platform for diverse opinions while also wanting users to feel safe and protected. We have recently published the detailed guidelines we use to implement these Community Standards. And we employ a highly trained team of reviewers who assess reports about potential violations of the standards with a high degree of consistency and accuracy.

We recognise that we sometimes make mistakes which lead to some content items being

left up or taken down in error. We are expanding the areas in which people can appeal the decisions we make to address these mistakes and we work hard to make continuous improvements to our systems to keep the number of errors as low as possible. We reject the idea in the question that this process of high quality professional review against publicly available standards constitutes "arbitrary censorship".

We give feedback to people whose content we have had to remove and we direct them to our Community Standards to help them better understand what they can and cannot share on our service. We do not remove Facebook pages without good cause. This may happen where the administrators of a page repeatedly post violating content in spite of the warnings we give them.

We understand that there are concerns about the potential impact of measures aimed at tackling false news on freedom of expression. We have described the way we are addressing the challenge of false news in this recent Hard Questions Blog. We are continuing to develop an approach that we hope will achieve the correct balance of preventing the spread of misinformation, while not stifling public discourse.

4. What are you doing to work with third party organisations to educate people to use the internet safely?

Keeping people safe online has always been a priority for Facebook. In 2009, we launched our Safety Advisory Board, made up of leading online safety organisations and experts from around the world. We have since built out a network of relationships with over 300 online safety organisations globally; and more recently we organised a committee of advisors with expertise in child development, online safety and media and child health.

We know our enforcement hasn't always been perfect. This is a difficult thing to get right and that's why we have made, and are continuing to make, major investments both in human expertise and in technology to more quickly help people who need our support and remove content that violates our policies. Below are some examples of how we work with third party experts to help educate our community on safety:

Safety Centre: We re-launched Safety Centre in 2016. The Safety Centre is used to help people feel safe and supported on our platform, as it walks people through the tools we offer to control your experience on Facebook, as well as numerous tips and resources. It is now mobile friendly, available in over 60 languages, includes step by step videos and resources from about 75 partners around the world. For more details, please see here.

Bullying Prevention Hub: Developed in partnership with the Yale Centre for Emotional Intelligence, the Bullying Prevention Hub is a resource for teens, parents and educators seeking support and help for issues related to bullying and other conflicts. It offers step-by-step plans, including guidance on how to start important conversations for people being bullied, parents who have had a child being bullied or accused of bullying, and educators who have had students involved with bullying. For more details, please see here.

Parents Portal: In November 2017, we launched a new "Parents Portal" where caregivers can come to learn some of the basics about Facebook, get tips on how to start a conversation about online safety with their children, and access external expert resources. The portal responds to feedback we have received from parents for more education around our safety policies, tools and resources. And just like our new Safety Centre, one of its key strengths is the access it offers to external expert safety partners. For more details, please see here.

Online Wellbeing: We launched an "Online Wellbeing" section in the Safety Centre in 2018 to provide people with more information on where to get more help regarding social resolution and suicide prevention. We also share how we work with organisations around the world to develop support options for people posting about suicide on Facebook, including support on how to reach out to a friend, as well as information on contacting help lines and tips about things they can do to help. For more details, please see here.

Youth Portal: In May 2018, we launched a new youth portal with resources for teens to empower them with information on the tools and policies they have for staying safe on Facebook as well as advice from their peers on a range of topics including how they have used the web to launch powerful campaigns. For more details, please see here.

Guides: We have worked with partners around the world to create safety resources and guides, for example:

- **Think Before You Share:** Together with MediaSmarts, we developed the Think Before You Share Guide that is designed for young people and contains tips about thinking before you post, not sharing passwords and how to resolve online issues. We have partnered with many European NGOs for this guide.
- **Help A Friend In Need:** Together with the Jed Foundation and the Clinton Foundation, we developed the Help A Friend In Need Guides which contain information about what to look out for on social media when your friend may be feeling down and how to get help. This has been widely launched with European NGOs.
- **Be Kind Online:** In partnership with Stonewall UK, Trevor Project and GLSEN we developed a guide to support LGBTIQ teens to encourage kindness online.

5. Why have you moved 1.5 billion users out of the reach of the GDPR? Aren't you violating the GDPR by doing so?

We welcome the GDPR, and, as of 25 May, operate in compliance with it. All users in the EU will continue to be provided with the Facebook service by Facebook Ireland, which remains the data controller for EU user data. Facebook Inc. will provide the Facebook service to people outside of Europe. It is not a violation of GDPR to provide our service in this manner; the GDPR includes specific provisions to ensure the application of the rules to people within the European Union, and we abide by those rules.

We will offer everyone who uses Facebook the same controls and settings, no matter where

they live. However, the GDPR creates some specific requirements that do not apply in the rest of the world, for example the requirement to provide contact information for the EU Data Protection Officer (DPO) or to specify legal bases for processing data. We are also looking to be more responsive to regional norms and legal frameworks going forward, and want to have the flexibility to work with local regulators, which is possible with this new model. At the same time, we are changing the provisions in our Facebook Inc. terms in our user agreements outside the United States to allow consumers in other countries to file lawsuits against Facebook in their home country, rather than in courts in the US. This transition was part of a continued effort to be locally responsive in countries where people use our services.

6. You explained that you will apply the GDPR principles globally. Will you afford the same level of protection to US and EU users?

Yes. As a part of our overall approach to privacy, we are providing the same tools for access, rectification, erasure, data portability and others to people in the US (and globally) that we provide in the European Union under the GDPR. The controls and settings that Facebook is enabling as part of GDPR include settings for controlling our use of face recognition on Facebook and for controlling our ability to use data we collect off Facebook Company Products to target ads. We recently began providing direct notice of these controls and our updated terms to people around the world (including in the US), allowing people to choose whether or not to enable or disable these settings or to consent to our updated terms.

The substantive protections in our user agreements offered by Facebook Ireland and Facebook Inc. are the same. However, there are certain aspects of our FB Ireland data policy that are specific to legal requirements in the GDPR— such as the requirement that we provide contact information for our EU Data Protection Officer (DPO) or that we identify the "legal bases" we use for processing data under the GDPR. Likewise, our Facebook Ireland terms and data policy address the lawful basis for transferring data outside the EU, based on legal instruments that are applicable only to the EU. And other provisions of the GDPR itself pertain to interactions between European regulators and other matters that are not relevant to people located outside of the EU.

7. Can you guarantee no manipulation on your platform ahead of the upcoming elections in Europe?

We support the goal of ensuring that elections are free and fair. We believe that our services can make a significant positive contribution to civic discourse in Europe and around the world. We see citizens using our platform to share their views on matters of public interest with their representatives and governments, and we see policy makers using our tools to engage directly with their constituents in ways that would not have been possible a decade ago.

But we also recognise that there can be abuse of our platform and have acknowledged that we have not done enough to identify and prevent this abuse in the past. In 2016, we were too slow to spot Russian interference on Facebook in the US Presidential election. We were not prepared for the coordinated misinformation operations we are now aware of. Since

then, we have made many significant investments to protect the integrity of elections by making these kinds of attacks much harder on Facebook and we are better than ever at finding and removing bad actors from the platform.

We are investing in more people. We are improving our technology, including AI, to remove fake accounts that are responsible for much of the false news, misinformation and bad ads on Facebook. This technology gets better with each election. We are working hard to avoid abuse and prevent bad actors from operating in the upcoming elections, including individual European elections and the European Parliament elections in 2019, with our efforts focused on five main areas: combating foreign interference, removing fake accounts, ads transparency, reducing the spread of false news and launching civic engagement products to make sure people have the right information ahead of an election. We are making it easier for our community to identify threats and we are working with governments and external partners to share information about threats in real-time, fill gaps on detailed threat detection and deterrence.

An especially important development is that we are going to make advertising more transparent, not just for political ads. Starting next month, people will be able to click “View Ads” on a Page and view all ads a Page is running on Facebook, Instagram and Messenger — whether or not the person viewing is in the intended target audience for the ad and whether or not the user follows the Page. This will be available for all the EU countries in the coming weeks. In addition, we are making pages more transparent by showing information about where the administrators of the page are based. Facebook also supports civic engagement and education by building tools that make it easier for people to spot abuse, have a voice and participate in the process. Lastly, we've created a training process for policy makers, politicians, candidates and their staff, to help them understand how their accounts could be abused, and to share advanced tips for safety and security during election periods.

The threats around elections change and we have to evolve with them. Security is not a problem you ever fully solve and we face sophisticated, well-funded adversaries who are constantly seeking new ways to get round our defences. Nobody can guarantee that all abuse will be eradicated, but we are committed to making the investments we need to stay ahead. We can best defend the integrity of elections when we work in collaboration with political parties, elections regulators, governments and academic experts. We very much look forward to continuing to build these collaborations, including with the European Parliament, over the coming months to do all we can to protect the upcoming elections together.

8. Will you commit from this year onwards to publish a list of your legal entities, number of employees, turnover, profit/losses, taxes paid, subsidies revived on a country by country basis?

We comply with all applicable company disclosure requirements. This means that, like any other company, we already publish regular company reports for all of our legal entities in line with the specific requirements of the country. We provide all required information to tax authorities which they may share with other tax authorities according to their agreed

protocols.

As these reporting requirements evolve, for example if new rules are agreed for the EU level, then we will adapt our reporting processes to match the new rules. Appropriate transition time should be given for companies to adequately implement them. We are not currently planning to publish information outside of the standard reporting requirements.

It may also be of interest to note that we are currently in the process of moving to a local selling structure. Further information on this can be found here. In simple terms, this means that advertising revenue supported by our local teams will no longer be recorded by our international headquarters in Dublin, but will instead be recorded by our local company in each country where we have a local sales office that supports local advertising. We believe this will provide more transparency to governments and policy makers around the world who have called for greater visibility over the revenue associated with locally supported sales in their countries.

9. How has Facebook's philosophy over sexism and discrimination evolved over time?

Our Community Standards govern everything which we believe has the potential to compromise the safety of our community, from bullying to hate speech and graphic violence, to spam and pornography.

We take sexual violence and exploitation on Facebook very seriously, and have been working for many years with a number of women's safety experts. For example NNEDV (the National Network to End Domestic Violence) in the U.S. have been part of our Safety Advisory Board for many years, and have guided our approach in this space. We remove threats of non-consensual sexual touching, credible threats, as well as content that advocates or glorifies sexual violence or exploitation. We take a particularly strong stance on anything that may sexualise children, or lead to the exploitation of minors. To protect victims and survivors, we also remove photographs or videos depicting incidents of sexual violence and images shared in revenge or without permissions from the people in the images.

Our definition of sexual exploitation includes solicitation of sexual material, any sexual content involving minors, threats to share intimate images, and offers of sexual services. Where appropriate, we refer this content to law enforcement. Offers of sexual services include prostitution, escort services, sexual massages, and filmed sexual activity.

Over the last few years we have also partnered with expert organisations across a number of countries, to understand local concerns, provide escalation points for sensitive situations, and promote responsible sharing as well as safety guides for women who may be victims of domestic violence. Since 2015 we have held a number of roundtables and safety events dedicated to the safety of women, including in pan-European events in Dublin, Berlin, London, Paris, Madrid and Amsterdam.

10. Can you promise that this data which you keep for security purposes is not used for other purposes, like targeted advertisements?

We collect and process data for a number of purposes, as set out clearly in our Data Policy. We look carefully at the purposes for the processing of each type of data to ensure that they are appropriate and lawful under the GDPR. We collect data for a range of processing purposes including safety and security but also for purposes such as personalisation of content (including ads), and measurement and analytics.

When we log data about people who are not registered Facebook users, we do not use these log records for targeted advertising, nor do we create profiles about non-users. These log records may be processed for safety and security purposes and for analytics purposes. For example we use log files to identify people who are trying to scrape Facebook data with repeated accesses from the same IP address. We may also provide analytics information that includes some information about all visitors to a page, but this reporting consists of summaries and does not describe any individual person.

11. Why was no information given to affected users when you first found out about Cambridge Analytica?

The information that surfaced in December 2015 reported that Dr. Kogan may have shared data that he obtained lawfully from users on Facebook's platform with a third party (Cambridge Analytica) in violation of our developer policies. Dr. Kogan's violation of our policies did not trigger a legal notification obligation by Facebook, both because the data shared with Dr. Kogan's app was authorised by users and because of the nature of the information itself — consisting of information people shared publicly or with their friends on Facebook (generally not passwords, financial data, or other data requiring notification under laws in place at the time).

Accordingly, our focus in December 2015 was to ensure that Dr Kogan and anyone with whom he had shared data promptly deleted all data. We retained an outside law firm to investigate and take action against Dr Kogan. We obtained certifications from Dr Kogan and others he shared data with assuring us that all variants of the data had been deleted. We also promptly removed Dr Kogan's app from the Facebook platform. An audit of Cambridge Analytica and the other parties involved would likely be the most effective way of seeking to determine what data was in fact shared and whether it was deleted at the time.

Because we are taking a broader view of our responsibilities that go beyond our legal obligations, we have since notified all people potentially impacted with a detailed notice at the top of their News Feed. In doing so, we have likely notified many people who did not have their data passed to Cambridge Analytica. Not only did we take an expansive methodology to identify users whose information may have been shared with Dr Kogan's app, but we also notified all potentially affected users outside the United States, despite Dr Kogan's statements that he only passed information relating to US users to Cambridge Analytica.

12. What is the legal situation regarding Facebook storing non-Facebook users' data?

When a person who is not a registered user of Facebook visits a site or app that uses our services and accepts the use of Facebook cookies (or similar technologies), we receive logs of this visit. This is an inherent feature of how the Internet works and occurs automatically by virtue of the fact that the person's device contacts Facebook's servers in order for the Facebook buttons and other features on those sites to work. The information received in this manner allows Facebook to identify a specific browser; however, when the person visiting the website or app is not a Facebook user, we do not receive any information that would allow us to identify the individual using that browser.

Facebook's processing of such data for non-users complies with all applicable laws. Our privacy policy (see here) explains in detail what we do with the information we receive, and makes clear that we may collect data from people away from Facebook who are logged out or don't have a Facebook account. Our Cookies Policy (see here) provides more detailed information about how and why we use cookies and the controls that people have. And we comply with applicable EU laws by obtaining consent from European users before dropping cookies that are not strictly necessary by displaying a cookie banner to every browser visiting Facebook for the first time to notify users about our cookie use as follows: "To help personalise content, tailor and measure ads and provide a safer experience, we use cookies. By clicking on or navigating the site, you agree to allow us to collect information on and off Facebook through cookies. Learn more, including about available controls: Cookie Policy."

In order for third parties to use our Facebook technologies in their websites or apps, it is also a contractual requirement that they do so in accordance with applicable laws and that where necessary they obtain valid consent or have another legal basis to share browser or app logs with Facebook from their service.

13. How does Facebook follow up to check compliance by third-party apps?

Our Platform Policy provides that "we can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app complies with our terms." However, audits are just one part of our broader enforcement program. We use a variety of tools to enforce Facebook policies against violating parties, including developers. We review tens of thousands of apps per year and regularly disapprove noncompliant apps as part of our proactive review process. We also use tools like cease and desist letters, account suspensions, letter agreements, and civil litigation. For example, since 2006, Facebook has sent over 1,150 cease-and-desist letters to over 1,600 targets.

14. Why did Facebook suspend 200 apps since the congressional hearings?

We have committed to investigate all the apps that had access to large amounts of information before we changed our platform policies in 2014 — significantly reducing the data apps could access. Where we have concerns about individual apps we will audit them — and any app that either refused or failed an audit would be banned from Facebook.

The investigation process is in full swing, and it has two phases. First, a comprehensive

review to identify every app that had access to this amount of Facebook data. And second, where we have concerns, we will conduct interviews, make requests for information — which ask a series of detailed questions about the app and the data it has access to — and perform audits that may include on-site inspections.

We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 have been suspended — pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and notify people via this website. It will show people if they or their friends installed an app that misused data before 2015 — just as we did for Cambridge Analytica.