DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

NOTICE OF INTENT

19 June 2018

To: Facebook Ireland Ltd

4 Grand Canal Square
Grand Canal Harbour
Dublin 2
Ireland

Facebook Inc
1610 Willow Road
Menlo Park, CA 94025

The above companies are collectively referred to in this Notice of Intent ("Notice") as "the Facebook Companies".

Introduction

1. The Information Commissioner ("the Commissioner") intends to issue the Facebook Companies with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The basis on which section 55A

continues to apply for the purposes of this Notice of Intent (notwithstanding the repeal of the DPA) is set out at paragraph 11 below.

2. The amount of the monetary penalty which the Commissioner intends to issue is £500,000.

3. As explained below, the Facebook Companies are joint data controllers in respect of the data processing to which this Notice relates, and hence the Commissioner considers that they are jointly and severally liable for the amount of the monetary penalty.

4. The intended monetary penalty arises out of a very serious data incident taking place before 25 May 2018 and affecting users whose personal data is processed on the Facebook platform ("Facebook Platform"). The total number of users worldwide who were affected by the incident has been estimated by the Facebook Companies themselves as being up to 87 million. Details of the incident are set out below.

5. The Commissioner considers that the Facebook Companies are and were at all material times joint data controllers of the personal data (at least) of data subjects who are resident outside of the USA and Canada and whose personal data is processed by or in relation to the operation of the Facebook Platform. This is on the basis that the Facebook Companies together do and did at all material times make decisions about how to operate the Facebook Platform in respect of the personal data of those data subjects. In other words, the Facebook Companies do and did at all material times jointly determine the purposes for which and the manner in which such personal data are and were processed.

6. The Commissioner considers that the Facebook Companies processed personal data in the context of a UK establishment. They did so where the personal data of any data subjects was processed in the context of

the operations of Facebook UK Limited ("Facebook UK"), company number 06331310, of 10 Brock Street, Regents Place, London NW1 3FG. The Commissioner's conclusion is based on the decision and reasoning of the CJEU in *Google Spain v AEPD* [2014] QB 1022, and the Court of Appeal of Northern Ireland in *CG v Facebook Limited and McCloskey* [2016] NICA 54.

7. The Commissioner considers, on this basis, that the Facebook Companies processed personal data in the context of a UK establishment, in respect of any individual on whose Facebook account any advertising appears which was sold or arranged by Facebook UK. This would include all personal data of data subjects who use Facebook.com in the UK; it is likely to include the personal data of other data subjects also.

8. For the reasons set out below, the Commissioner considers that:

   (1) The Facebook Companies unfairly processed personal data, in breach of the first data protection principle ("DPP1") set out in Schedule 1 to the DPA; and

   (2) The Facebook Companies failed to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data, in breach of the seventh data protection principle ("DPP7") set out in Schedule 1 to the DPA.

The Facebook Companies breached DPP1 and DPP7, in respect of the processing of personal data that took in the context of a UK establishment, as explained above. The Facebook Companies thereby acted in breach of section 4(4) of the DPA, which at all material times required data controllers to comply with the data protection principles in

relation to all personal data in respect of which they were the data controller.

9. The Commissioner's preliminary view is that, in all the circumstances, each of these failures constituted a serious contravention by each of the Facebook Companies of DPP1 and DPP7. The Commissioner further considers that the conditions for issuing a monetary penalty are satisfied, that it is appropriate to issue such a penalty in this case, and that the amount of £500,000 is reasonable and proportionate.

10. This Notice of Intent is served under section 55B of the DPA. It explains the grounds on which the Commissioner intends to issue the monetary penalty. The Commissioner will consider any representations from the Facebook Companies before reaching a final decision on this matter.

11. The DPA was repealed with effect from 25 May 2018 by the Data Protection Act 2018. However, sections 55A, 55B, 55D and 55E of the DPA continue to apply for the purposes of the present case, since the Commissioner considers it appropriate to serve this Notice of Intent in respect of contraventions of section 4(4) of the DPA taking place before 25 May 2018: see Data Protection Act 2018, Schedule 20, Part 7, paragraph 38(1)(c).

Legal framework

12. The DPA implemented European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive.

13. The Facebook Companies are joint data controllers of personal data, as explained above. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

14. Schedule 1 of the DPA contains the eight data protection principles. For the purposes of this Notice, DPP1 and DPP7 are relevant.

15. DPP1 stipulates as follows:

> *Personal data shall be processed fairly and lawfully in in particular, shall not be processed unless –*
>
> *(a) at least one of the conditions in Schedule 2 is met, and*
> *(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

16. DPP7 stipulates as follows:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

17. As regards DPP7, the interpretative provisions in Part II of Schedule 1 to the DPA provide that:

> *9. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—*
> *(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*
> *(b) the nature of the data to be protected.*
>
> *10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.*

11. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—
(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
(b) take reasonable steps to ensure compliance with those measures.

12. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—
(a) the processing is carried out under a contract—
(i) which is made or evidenced in writing, and
(ii) under which the data processor is to act only on instructions from the data controller, and
(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

18. Section 55A of the DPA empowers the Commissioner to issue monetary penalties. The relevant provisions are as follows:

(1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—
(a) there has been a serious contravention of section 4(4) by the data controller,
(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller—
(a) knew or ought to have known —
(i) that there was a risk that the contravention would occur, and
(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but
(b) failed to take reasonable steps to prevent the contravention.

19. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

20. The Commissioner has issued and published statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties.

The Commissioner's investigation

21. The Commissioner has commenced an investigation into the use of data analytics for political purposes. The Commissioner's investigation is aimed at assessing the data processing practices of, amongst others, political parties and campaigns, data companies, and social media platforms. The investigation extends to the ways in which companies operating internationally deploy such practices when processing data in the context of an establishment in the United Kingdom.

22. The Facebook Platform is a social media platform that has been used by political parties and campaigns. The Facebook Platform, and the processing of personal data by the Facebook Companies in connection with the operation of that Facebook Platform, has therefore been brought within the scope of the Commissioner's investigation.

23. An initial letter was sent to the Facebook Companies on 23 August 2017, and the Commissioner has carried out extensive further investigations thereafter in respect of those companies. The matters set out in this Notice are based on the evidence obtained by the Commissioner in the course of that investigation.

Factual circumstances relevant to the contravention

24. The Facebook Companies, throughout the period of time that is relevant to this Notice, have permitted third parties to operate applications, or "apps", in conjunction with the Facebook Platform. Further, the Facebook Companies, throughout the period of time that is relevant to this Notice, have permitted such third parties to obtain personal data about those users of the Facebook Platform who install the third party's app. Since the launch of Facebook's Platform in May 2007, the Facebook Companies have also permitted such third parties to obtain personal data about users of the Facebook Platform who do not themselves install the third party's app, but whose Facebook friends install that app.

25. In 2013, an individual named Dr. Aleksandr Kogan created an app that subsequently became known as "thisisyourdigitallife" ("the App") for use in conjunction with the Facebook Platform. Dr. Kogan acted both in his own capacity and by means of his company, Global Science Research Limited ("GSR"). The Facebook Companies permitted Dr. Kogan and/or GSR to operate the App in conjunction with the Facebook Platform, with effect from November 2013. The App was therefore operating on Graph API v.1.0 at this time.

26. As a result, Dr. Kogan and/or GSR were able to obtain personal data both from individuals who opted to use the App, and from Facebook friends of those users.

27. The App utilised Facebook Login in order to request permission from users of the App to access certain data from their Facebook accounts. The App was designed to and was able to obtain the following categories of information from individuals who opted to use the App:

- Their public Facebook profile, including their name and gender.

- Birthdate.
- "Current city", if the user had chosen to add this information to their profile.
- Photographs in which the users were tagged.
- Pages that the users had liked.
- Posts on the users' timeline.
- News feed posts.
- Friends lists.
- Email addresses.
- Facebook messages.

In relation to Facebook messages, it is unclear whether the information obtained by the App was confined to the parties who exchanged messages, or whether it also included the content of the messages.

28. By means of the information obtained from users of the App, the App generated personality profiles for those users.

29. To the extent that the App had access to the identity of those who had exchanged Facebook messages with a user of the App, or to the content of such messages, the individuals who had exchanged such messages with users of the App: were not informed that the App was being given access to such information; and were not asked to consent to such access.

30. The App also requested permission from users of the App to access the following categories of data about their Facebook friends:

- Public profile data, including name and gender.
- Birthdate.
- "Current city", if the friends had chosen to add this information to their profile.

- Photographs in which the friends were tagged.
- Pages that the friends had liked.

The App was therefore designed to and was able to obtain an extensive range of data about the Facebook friends of the App's users.

31. Where the App collected data about the Facebook friends of the App's users, those friends were not informed that the App was being given access to that data, and were not asked to consent to such access.

32. In April 2014, the Facebook Companies introduced changes to the Facebook Platform, which reduced the ability of apps to access information both about their users and about the Facebook friends of their users. For pre-existing apps, there was a one year grace period (until May 2015) before they were subject to these new limitations, and so they were able to continue to collect the data of users' friends as before for up to a year following the changes.

33. Dr Kogan requested to migrate the App to V2 of the Graph API Platform prior to the end of the grace period. The App was subject to review on 6 May 2014 and Facebook rejected Dr Kogan's request for extended permissions the following day.

34. After May 2014, the App ceased to have access to detailed information about the friends of its users, and had access to a more limited set of information about its users. However, when the limitations took effect in May 2015 following the one year grace period, application developers including Dr Kogan and GSR were able to retain detailed information about users of their apps and their friends that they had previously collected via their apps. The Facebook Companies did not at that point require them to delete such data, or any of it.

35. The App remained in operation on the Facebook Platform until December 2015.

36. The App was used by some 300,000 Facebook users worldwide. Because the App was able to collect data about the Facebook friends of its users, the total number of individuals about whom the App collected personal data has been estimated by the Facebook Companies as being up to 87 million worldwide. The number of UK Facebook users who used the App has been stated by the Facebook Companies to be 1,040 (though the Facebook Companies have also stated that 1,765 individuals in Great Britain used the App). The total number of UK Facebook users about whom the App collected personal data has been estimated by the Facebook Companies as being at least 1 million.

37. Dr. Kogan and/or GSR shared such personal data (both about users of the App, and about their Facebook friends), and/or data derived from such data, with the following companies:

- Toronto Laboratory for Social Neuroscience, University of Toronto
- Eunoia Technologies, Inc: this is a marketing company based in Canada, and may have been associated with SCL Elections Limited and Cambridge Analytica
- SCL Elections Limited (which controls Cambridge Analytica)

At least some of the data shared with these companies is likely to have been used in connection with or for the purposes of political campaigning.

38. The Facebook Companies operated a Platform Policy in relation to the operation of apps. The Facebook Companies took no steps, or no sufficient steps, to ensure that the App operated consistently with the Platform Policy. For instance, the Facebook Companies did not review

the terms and conditions governing the relationship between Dr. Kogan and/or GSR and the users of the App in order to check that they were consistent with the Platform Policy. Nor did the Facebook Companies establish any system under which such a review would have taken place.

39. The Facebook Companies have admitted that the way in which the App was operated was in breach of the Platform Policy in at least the following respects:

- In accordance with section 3.3 of the Platform Policy, data obtained about friends of users of the App should have been utilised solely to augment the experience of those users within the App. Instead, in breach of section 3.3, such data was used by Dr. Kogan and/or GSR for their own purposes.

- In breach of section 3.9 of the Platform Policy, Dr. Kogan and/or GSR sold to third parties personal data that was collected by the App.

- In breach of section 3.10 of the Platform Policy, Dr. Kogan and/or GSR transferred to third parties personal data that was collected by the App.

- The App requested permission from users to obtain personal data that the App itself did not need. This was in breach of section 7.4 of the Platform Policy.

40. Further, on 6 May 2014 Dr. Kogan gave an undertaking to the Facebook Companies ("the Undertaking") that the App was being used for research purposes only, and not for commercial purposes. The Facebook Companies took no steps, or no sufficient steps, to ensure that the App was being operated consistently with the Undertaking.

41. In breach of the Undertaking, Dr. Kogan and/or GSR marketed research on a commercial basis, derived from personal data collected by the App.

42. The Facebook Companies did not become aware that the App was being operated in breach of the Platform Policy and the Undertaking, until an article relating to the App was published in the Guardian Newspaper on 11 December 2015. Only at that point did the Facebook Companies terminate the App's access rights to the Facebook Login API, and commence an investigation into the operation of the App.

The contravention

43. By reason of the matters set out above, the Facebook Companies acted in breach of DPP1 and DPP7.

Breach of DPP1

44. In breach of DPP1, the Facebook Companies unfairly processed the personal data of users of the Facebook Platform, including: those who were users of the App; those who exchanged Facebook messages with users of the App; and those who were Facebook friends with users of the App.

45. The Facebook Companies permitted the App to operate in such a way that it collected personal data about Facebook friends of users of the App, without those Facebook friends being informed that such data was being collected, and without them being asked to consent to such data collection. The Facebook Companies did not attempt to prevent the App

from collecting data in this manner; for instance, such data collection was not prohibited by the Platform Policy. By permitting the App to operate in this way, the Facebook Companies unfairly processed the personal data of the Facebook friends of users of the App. Further, to the extent that such processing of personal data was purportedly based on consent, any such consent was invalid and ineffective, since it was not freely given, specific, or informed: see the definition of "consent" in Directive 95/46/EC, Article 2(h).

46. The Facebook Companies have asserted, in the course of the Commissioner's investigation, that data about users' Facebook friends was only collected by the App if the privacy settings adopted by those Facebook friends permitted such collection to take place. Even if this is the case, it is not sufficient to render such processing fair.

- It is now apparent that, for at least part of the period during which the App had access to the Facebook Platform, extensive information about Facebook users could be collected by an app, as a result of other Facebook users choosing to use that app: see paragraph 30 above. During the period when the App was permitted to access the Facebook Platform, the Facebook Companies failed to provide adequate information to Facebook users that this could occur, and as to the steps that they needed to take to prevent this. Individuals would not reasonably have expected their personal data to be collected in this way merely because of a choice made by other individuals to use a particular app.

- It was unfair for the Facebook Companies to rely on a Facebook user's privacy settings as enabling apps installed by the user's Facebook friends to collect extensive personal data from the user's account (of the type set out at paragraph 30 above). The Facebook Companies ought instead to have ensured that, before access to such personal

data took place, the Facebook user: was informed that the app wished to access such personal data; was told how such data was sought, and how it would be used; and was given the opportunity to give or withhold their consent for such access.

47. To the extent that the App collected information about the Facebook messages of users of the App, the individuals who had exchanged such messages with users of the App: were not informed that such information was being collected; and were not asked to consent to the collection of such information. To the extent that the App collected information in this way, the Facebook Companies permitted it to do so. It was not a breach of the Platform Policy for the App to operate in this way. By permitting the App to operate in this way, the Facebook Companies unfairly processed the personal data of the individuals who had exchanged Facebook messages with users of the App.

48. By reason of the matters set out at paragraphs 45 to 47 above:

- any consent purportedly given by the Facebook friends of users of the App, so as to permit the App to collect their personal data, was not freely given, specific or informed;

- hence any such consent was ineffective and invalid and did not provide a lawful basis for the processing in question.

49. Further, the Facebook Companies permitted the App to operate on the Facebook Platform, in circumstances where the Facebook Companies failed to take any steps, or any sufficient steps, to monitor whether the App was being operated in breach of the Platform Policy. The Facebook Companies thereby unfairly processed the personal data of: users of the App; Facebook friends of users of the App; and individuals who exchanged Facebook messages with users of the App. In the case of all

of these groups, Facebook unfairly exposed them to a risk that their personal data would be used in breach of the Platform Policy.

50. The Facebook Companies acted in breach of DPP7, by failing to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data of: users of the App; Facebook friends of users of the App; and individuals who exchanged Facebook messages with users of the App.

51. To the extent that the personal data of such individuals was processed by Dr. Kogan and/or GSR, such processing was both unauthorised and unlawful.

- The processing was unauthorised, in that it was inconsistent with the basis on which the Facebook Companies permitted Dr. Kogan and/or GSR to obtain access to personal data of which they were data controller. In particular, such processing was in breach of the Platform Policy and the Undertaking, as explained above.

- The processing was unlawful, in that it constituted unfair processed by Dr. Kogan and/or GSR of the personal data of those individuals.

52. The Facebook Companies took no steps, or no adequate steps, to guard against such unauthorised or unlawful processing.

- The Facebook Companies did not review the terms and conditions offered to users of the App, in order to assess whether those terms and conditions were consistent with the Platform Policy. Nor did the Facebook Companies establish any system for such monitoring of the content of the terms and conditions to take place. The terms and conditions that the App offered to its users were not provided to the

Facebook Companies until 14 December 2015 (after the start of the investigation referred to at paragraph 40 above).

- The Facebook Companies took no steps to monitor whether the App was being operated in a manner consistent with the Platform Policy and the Undertaking.

53. The fact that the Facebook Companies failed to take any or any adequate steps in this regard, is confirmed by the fact that it was not until an article was published in the *Guardian* newspaper on 11 December 2015 that the Facebook Companies became aware that the App had been operated in breach of the Platform Policy and the Undertaking.

The issuing of a monetary penalty

54. The Commissioner's preliminary view is that the conditions for imposing a monetary penalty notice have been met in this case.

55. The Commissioner considers that this contravention was serious.

- It affected a very large number of individuals.

- As a result of the contravention, a very substantial volume of personal data was shared with third parties by Dr. Kogan and/or GSR, without the relevant data subjects being made aware of this or being given the opportunity to consent to the data sharing.

56. The Commissioner considers that this contravention was of a kind likely to cause substantial distress. Individuals were likely to be distressed by the fact that the Facebook Companies had permitted and/or enabled the App to operate in the manner set out above, and had failed to take

adequate steps to protect their personal data. The extensive disclosure of personal data to third parties, without the data subjects being aware of such disclosure or being able to disclose it, was also likely to cause distress. This is particularly the case given that at least some of the data shared with these third parties is likely to have been used in connection with or for the purposes of political campaigning, a use which would have fallen outside any reasonable expectation of the data subjects. The nature of such distress and/or the number of individuals likely to be distressed, were sufficient to establish that the distress was substantial.

57. The Commissioner considers that the Facebook Companies knew or ought reasonably to have known that there was a risk that the contravention would (a) occur, and (b) be of a kind likely to cause substantial distress. She further considers that the Facebook Companies failed to take reasonable steps to prevent such a contravention, in that:

(1) The Facebook Companies, viewed collectively, are a large, well-resourced and experienced data controller. They should have been aware of the risks .

(2) The Facebook Companies had ample opportunity over a long period of time to implement appropriate technical and organisational measures in respect of the matters set out above, but failed to do so.

58. The Commissioner's preliminary view is therefore that the statutory conditions for issuing a monetary penalty have been met in this case. She has considered all the circumstances and has reached the preliminary view that it is appropriate to issue a monetary penalty in this case.

The amount of the monetary penalty which the Commissioner intends to issue

59. The Commissioner has taken into account her underlying objective in imposing a monetary penalty notice, namely to promote compliance with the DPA. She considers that, given the nature, seriousness and potential consequences of the contravention arising in this case, that objective would not be adequately served by an unduly lenient penalty.

60. When they became aware of the inappropriate access to users personal data, and its extent, in 2015 the Facebook Companies began to take steps to ensure that accessed personal data was deleted by those who had it in their possession. Those measures were however ineffective and slow, particularly in the context where there were concerns about the integrity of the App developer's actions. The Facebook Companies did not follow up with the parties involved quickly, allowing them months to certify that the data had been deleted. The Facebook Companies did not challenge statements made by SCL Group in its return which in effect rendered their certification useless, and did not follow up with a proposed audit of the systems of recipients of the data, backed by suspension from its platform, until 2018. This poor response in the context of the Facebook Companies' scale and resources is an aggravating factor considered by the Commissioner.

61. The Commissioner has also taken into account the following factors:

    (1) Once the Facebook Companies became aware of the matters raised in the Guardian article of 11 December 2015, they immediately terminated the App's access to the Facebook Platform, and investigated the way in which the App had been operated.

(2) During the course of the Commissioner's investigation the Facebook Companies have been co-operative, including by providing detailed answers to successive Information Notices served by the Commissioner.

62. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of £500,000 is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

63. The Commissioner has considered evidence of the Facebook Companies' financial position. She does not consider that the payment of a penalty of the above amount would cause the Facebook Companies undue hardship.

Conclusion and next steps

64. The Commissioner intends to make her final decision as to whether to serve a monetary penalty for such amount on or after 18 July 2018. If the Facebook Companies wish to make any representations in response to this Notice, they must do so before that date. A sheet explaining the procedure for making representations is attached to this Notice as Annex 1.

65. The Commissioner will make her final decision once she has considered any such representations from the Facebook Companies.

Dated 19 June 2018

Signed [redacted]

Elizabeth Denham
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ico.
Information Commissioner's Office

ANNEX 1

DATA PROTECTION ACT 1998

REPRESENTATIONS IN RESPONSE TO A NOTICE OF INTENT

The Information Commissioner has power under sections 55A and 55B of the Data Protection Act 1998 to serve a monetary penalty notice on a data controller. Before she exercises this power the Commissioner wishes to take account of all the relevant facts and arguments.

This Notice of Intent is to enable the person affected to put his side of the case. The Commissioner's intentions are set out in the accompanying Notice of Intent. If you wish to make representations on those matters you have an opportunity to do so. The closing date for this is in the accompanying Notice of Intent.

Representations should be made in writing. You may wish to comment on the facts and views set out by the Commissioner or to make general remarks on the case and enclose documents or other material. A data controller should also inform the Commissioner if any confidential or commercially sensitive information should be redacted from a monetary penalty notice.

All representations will be carefully considered by the Commissioner before a final decision is made.

Representations should be sent to Emma Bate, General Legal Counsel, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by email to [redacted]