From:	[redacted] (CNECT)	Protection of personal data Art 4(1)(b)
To:	SPANOU Despina (CNECT); [redacted] (CNECT); [redacted] (CNECT); [redacted] (CNECT); [redacted] (CNECT)	
Cc:	CNECT H1	
Subject:	Meeting w/ Facebook representatives on the ePrivacy Regulation (Monday 27th of March)	
Date:	mardi 28 mars 2017 18:26:31	
Attachments:	image001.gif	

Dear All,

Yesterday we had a meeting with representatives of Facebook on the proposal for a Regulation on ePrivacy.

In a nutshell, Facebook expressed concerns about various articles of the proposed ePrivacy Regulation, including Arts 5- 7 (confidentiality of communications), Article 8 (use of processing capabilities of terminal equipment) and 10 (browser settings).

Please find below detailed notes of the briefing, which includes the points made by Facebook (not our responses).

Articles 5 to 7 [Confidentiality of communications]

- Facebook's understanding of these articles is that they only cover ECS providing communications.
- *According to Facebook*, Messenger is not a messaging service (sic). It is much more than that because it can notify you about an event which was mentioned during a conversation, it can suggest new friends based on the content of discussions, etc. In short, Messenger provides many value-added services.
- As a consequence of this, asking for consent would be disproportionately cumbersome and not user-friendly.

Article 10 [Browser settings]

- The Proposal's answer to the cookie issue poses a threat to Facebook's business model.
- Under Article 10, users will be asked to make a choice upon installation of their internet browsers. But the way browsers inform users may prove to be problematic. For example, the explanations provided under each setting could potentially nudge the users towards blocking of all third-party services.
- This will certainly lead the vast majority of the users to completely turn off cookies and other identifiers.
- Contrary to centralised settings, cookie banners have the benefit of being contextual; users can therefore see in what context the cookies are asked, and act accordingly. Facebook acknowledges cookies banners is a 'broken system', but they believe a different solution should be envisaged than a centralised setting built into the browsers.
- According to them, the Proposal does not effectively get rid of cookie banners, because users will still be prompted with banners for exceptions to be made ('add to white list') to the general setting of the browser. Thus, the Proposal is not a real improvement for the end-users: new banners and requests will appear.
- Facebook proposes to leave to the browsers manufacturers the decision on the

browser settings and how to inform users about such settings. They claim that the market will provide privacy friendly settings. Facebook referred to Apple's Safari, which already empowers its users to excludes all third-party cookies. Apple didn't wait for the Proposal to implement this function, because such privacy by design corresponds to the firm's general policy on privacy. In other words, Safari is calibrated to the traditional target audience of Apple ("if you want privacy, choose an iPhone").

- In Facebook's view, this suggests that there is no need for a Regulation: the audience will determine on its own which privacy settings or policy it adheres to, and choose the ECSs accordingly.

Article 8(1) [Use of processing capabilities of terminal equipment]

- Facebook considers that the European Commission should include an exception allowing for some third-party cookies without consent, e.g. to allow at the very least cookies used to calculate the impact of advertisements (number of views).
- The Proposal doesn't take into account the short span of attention of end-users, and the fact that the vast majority of them won't read the explanations regarding the consequences of blocking all third-party cookies.
- Facebook wishes the legal basis for processing under the ePR to be enlarged to the legal grounds under the GDPR.
- It believes legitimate interest to be a sufficient ground for processing.
- Moreover, legitimate interest offers flexibility: it can be adapted to the context (cf. Recital 47 GDPR), while consent is deemed to be too rigid ("Many different services require as many different interactions with the users").
- Another solution, in the eyes of Facebook, would be *consent that is not purpose related*, e.g. on iOS and Android, where allowing applications to use your location covers a great variety of purposes (it's either on or off for a particular app; never purpose specific). The contrary would, once again, result in a notice-fatigue of users, who would need to stipulate each time for what specific purpose an application should use its camera, its location, etc.

Best regards,

[redacted]

Personal data protection Art 4(1)(b)

on behalf of

[redacted]

[redacted]

European Commission
DG CONNECT
Cybersecurity & Digital Privacy- Unit H1

Av. De Beaulieu [redacted]
B-1160 Brussels/Belgium

Tel: +32. 2. [redacted]
Mob: +32 460 [redacted]

+32 474

@ec.europa.eu