Media Update

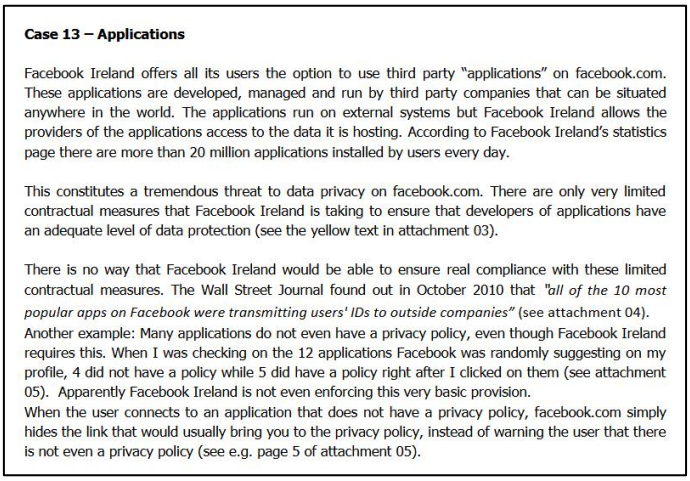
Max Schrems: Facebook knew about later "*Cambridge Analytica*" problem since 2011 – but said data sharing with questionable apps is perfectly legal

Lawyer for Facebook in 2012 argued data sharing allowed under privacy policy
Irish Privacy Regulator saw "satisfactory response" in 2012 "Audit" of Facebook

Max Schrems (chairman of noyb.eu) is surprised by Facebook's reaction on the Cambridge Analytica scandal: "*Facebook has millions of times illegally distributed data of its users to various dodgy apps - without the consent of those affected. In 2011 we sent a legal complaint to the Irish Data Protection Commissioner on this. Facebook argued that this data transfer is perfectly legal and no changes were made. Now after the outrage surrounding Cambridge Analytica the Internet giant suddenly feels betrayed seven years later. Our records show: Facebook knew about this betrayal for years and previously argues that these practices are perfectly legal.*"

Document 1: Legal Complaint on Problem with "Apps"

In a complaint filed with the Irish Data Protection Authority in the summer of 2011 (screenshot below), Max Schrems described exactly those two issues that now led to the "Cambridge Analytica" scandal: First, apps could also retrieve data from "friends" of users installing an app without the friends' consent. Second, it was completely unclear which apps received this data and whether they would ever adhere to data protection regulations. Facebook had no control here. Both blatantly violate European data protection law, which was already applicable on Facebook in 2011 because it had its head office in Ireland.



Case 13 – Applications

Facebook Ireland offers all its users the option to use third party "applications" on facebook.com. These applications are developed, managed and run by third party companies that can be situated anywhere in the world. The applications run on external systems but Facebook Ireland allows the providers of the applications access to the data it is hosting. According to Facebook Ireland's statistics page there are more than 20 million applications installed by users every day.

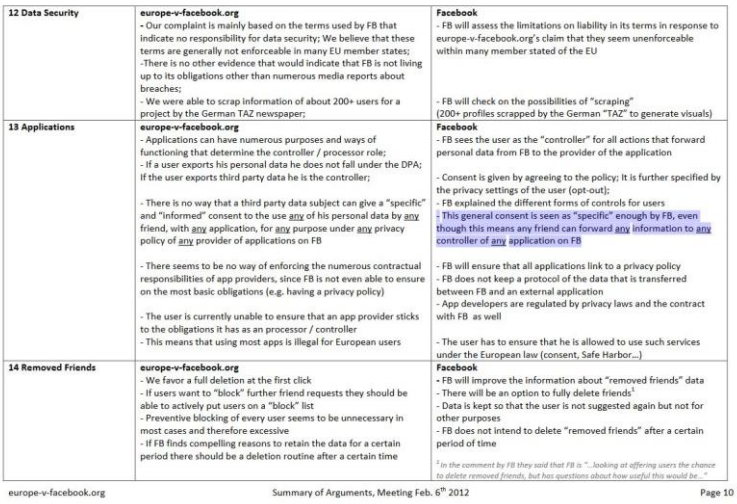
This constitutes a tremendous threat to data privacy on facebook.com. There are only very limited contractual measures that Facebook Ireland is taking to ensure that developers of applications have an adequate level of data protection (see the yellow text in attachment 03).

There is no way that Facebook Ireland would be able to ensure real compliance with these limited contractual measures. The Wall Street Journal found out in October 2010 that *"all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies"* (see attachment 04).
Another example: Many applications do not even have a privacy policy, even though Facebook Ireland requires this. When I was checking on the 12 applications Facebook was randomly suggesting on my profile, 4 did not have a policy while 5 did have a policy right after I clicked on them (see attachment 05). Apparently Facebook Ireland is not even enforcing this very basic provision.
When the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy (see e.g. page 5 of attachment 05).

Document 2: Facebook 2012: "Users gave consent to data sharing"

In a seven-hour conversation at Vienna Airport in 2012, representatives of Facebook and Max Schrems also debated about the legal status of apps. As the protocol of this conversation (page 10, screenshot below) shows, Facebook argued that it's privacy policy would legitimize this data transfers. Facebook said that all users agreed to unknown apps getting their data with no serious limitations.

Schrems: "*Such a blank approval is completely invalid under European law. How should a user know which friend has installed a windy app that is hosted somewhere in China and what happens to my data? But Facebook continued to provide data to all those questionable apps.*"



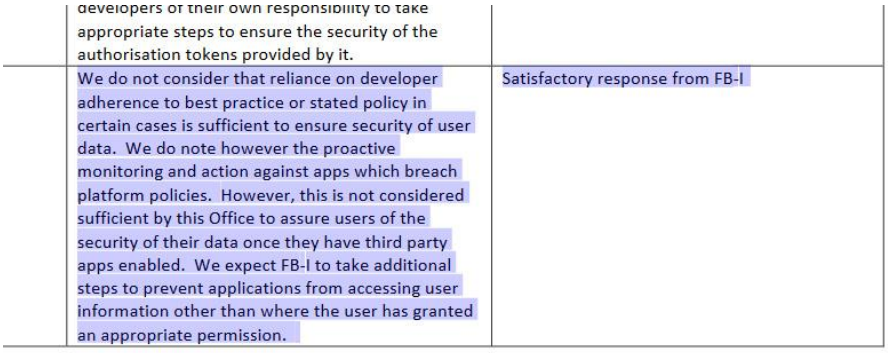
12 Data Security	**europe-v-facebook.org** - Our complaint is mainly based on the terms used by FB that indicate no responsibility for data security; We believe that these terms are generally not enforceable in many EU member states; -There is no other evidence that would indicate that FB is not living up to its obligations other than numerous media reports about breaches; - We were able to scrap information of about 200+ users for a project by the German TAZ newspaper;	**Facebook** - FB will assess the limitations on liability in its terms in response to europe-v-facebook.org's claim that they seem unenforceable within many member stated of the EU - FB will check on the possibilities of "scraping" (200+ profiles scrapped by the German "TAZ" to generate visuals)
13 Applications	**europe-v-facebook.org** - Applications can have numerous purposes and ways of functioning that determine the controller / processor role; - If a user exports his personal data he does not fall under the DPA; If the user exports third party data he is the controller; - There is no way that a third party data subject can give a "specific" and "informed" consent to the use any of his personal data by any friend, with any application, for any purpose under any privacy policy of any provider of applications on FB - There seems to be no way of enforcing the numerous contractual responsibilities of app providers, since FB is not even able to ensure on the most basic obligations (e.g. having a privacy policy) - The user is currently unable to ensure that an app provider sticks to the obligations it has as an processor / controller - This means that using most apps is illegal for European users	**Facebook** - FB sees the user as the "controller" for all actions that forward personal data from FB to the provider of the application - Consent is given by agreeing to the policy; It is further specified by the privacy settings of the user (opt-out); - FB explained the different forms of controls for users - This general consent is seen as "specific" enough by FB, even though this means any friend can forward any information to any controller of any application on FB - FB will ensure that all applications link to a privacy policy - FB does not keep a protocol of the data that is transferred between FB and an external application - App developers are regulated by privacy laws and the contract with FB as well - The user has to ensure that he is allowed to use such services under the European law (consent, Safe Harbor...)
14 Removed Friends	**europe-v-facebook.org** - We favor a full deletion at the first click - If users want to "block" further friend requests they should be able to actively put users on a "block" list - Preventive blocking of every user seems to be unnecessary in most cases and therefore excessive - If FB finds compelling reasons to retain the data for a certain period there should be a deletion routine after a certain time	**Facebook** - FB will improve the information about "removed friends" data - There will be an option to fully delete friends[1] - Data is kept so that the user is not suggested again but not for other purposes - FB does not intend to delete "removed friends" after a certain period of time [1] In the comment by FB they said that FB is "...looking at offering users the chance to delete removed friends, but has questions about how useful this would be..."

europe-v-facebook.org Summary of Arguments, Meeting Feb. 6th 2012 Page 10

Document 3: Irish DPC saw "satisfactory response" in 2012 audit of Facebook

The Irish DPC was fully informed about these events, which became a scandal seven years later. In the DPC's report in response to Max Schrems complaints, however, the DPA made only superficial suggestions for improvement. For example, users should get better information - but the illegal data flow to apps was not stopped.

In the final "Re-Audit" (page 29, screenshot below) the Irish regulator found a "satisfactory response" by Facebook. Only two years later an App stripped the data of 50 million profiles from Facebook and forwarded them to Cambridge Analytica.



	developers of their own responsibility to take appropriate steps to ensure the security of the authorisation tokens provided by it.	
	We do not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. We do note however the proactive monitoring and action against apps which breach platform policies. However, this is not considered sufficient by this Office to assure users of the security of their data once they have third party apps enabled. We expect FB-I to take additional steps to prevent applications from accessing user information other than where the user has granted an appropriate permission.	Satisfactory response from FB-I

As of May 25, 2018: US$ 1.6 billion penalty and noyb.eu

Schrems: *"This case shows again perfectly what has not worked so far in European data protection. A large corporation knowingly ignores European law and illegally passes on data. The regulator in Ireland is looking away and the data of millions of users are landing at Cambridge Analytica to influence our elections."*

If this happened after May 25 this year, Facebook could face a fine of up to $ 1.6 billion Dollars (4% of global sales in 2017). These are the penalties according to the new EU General Data Protection Regulation (DSGVO) that will apply from 25 May 2018.

Schrems: "*Even after the new EU privacy law comes into force, we need someone to cover these cases - as I did in 2011 - and bring them to the courts. For this we have now founded the European enforcement association called noyb.eu. As soon as we are fully funded, we will use lawyers and technicians to expose such violations and bring in lawsuits and complaints. We have to ensure that the 'big European data protection lie is brought to an end: We have laws but companies do whatever they want as there is no enforcement.* "

========

Documents (free to use):

Original complaint from 2011: PDF
Protocol of positions during a meeting with Facebook in 2012 (page 10): PDF
"Audit" of the Irish DPC from 2012 (page 86 on apps) : PDF
"Review" by the irish DPC from 2012 (page 29 on apps): PDF

Questions?

...via phone: +43 664 4602350
...via email: media@noyb.eu