#	Inhalt	Quelle
1	**Facebook failed to be accountable for the user information under its control.** Facebook did not take responsibility for giving real and meaningful effect to the privacy protection of its users. It abdicated its responsibility for the personal information under its control, effectively shifting that responsibility almost exclusively to users and Apps. Facebook relied on overbroad consent language, and consent mechanisms that were not supported by meaningful implementation. Its purported safeguards with respect to privacy, and implementation of such safeguards, were superficial and did not adequately protect users' personal information. The sum of these measures resulted in a privacy protection framework that was empty.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
1	»[…] because I think they realise that the platform has been mined left and right by thousands of others«. Dr Kogan's interpretation of what happened seems to be supported by the Six4Three evidence. Facebook was violating user privacy because, from the beginning, its Platform had been designed in that way.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 39. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
1	Elizabeth Denham told the Committee that the ICO »found their business practices and the way applications interact with data on the platform to have contravened data protection law.«	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 21. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
1 & 18 & 21	It should be noted that several other prominent platforms, like Android and IOS, allow access to friend (contact) data with user permission. Like us, those platforms has policies about the use of data, but misusing contacts gathered knowingly from a phone is also not a »breach«. In 2015, we updated our APIs to remove the ability to see this kind of friend data. This was controversial with app developers at the time, but was the right decision to increase privacy and reduce the chance of abuses like that. The ability to get friend data via API, with the permission of the user, was documented in our terms of service, platform documentation, the privacy settings, and the screen used to login	Wagner. (2018). Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. vox.com. https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data

1 & 3 & 17	From the technical implementations that I saw regarding the whitelisted partners—the whitelisted apps—they were incredibly hacky and thrown together very haphazardly. It seemed as if a business development person and an engineer implemented a feature quickly. For example, in order to whitelist an app, all they did was say it was pre-installed for all users. That was the workaround, instead of creating a new oversight regime or a new API specifically for those apps. They essentially just added a flag to the database that said it is a pre-installed app, so it gets permissions by default, so it can skip over the consent process. That is very hacky. […] . That makes it very hard to regulate and it makes it hard to oversee internally. As a result, there are engineers just running in the direction set for them—that leadership has set—and I am not sure that leadership is giving guidance to say, »No, you know what? This is a priority. User privacy is a priority,« or »Data use is a priority.«	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4349, Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.
1 & 16 & 21	However, therewere »whitelisted« apps that could still access user data without permission and which, according to Ashkan Soltani, could access friends' data for nearly a decade before that time. Apps were able to circumvent users' privacy of platform settings and access friends' information, even when the user disabled the Platform. This was an example of Facebook's business model driving privacy violations.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 29. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
2	A November 2013 email discussion reveals that Facebook was managing 5,200 whitelisted apps [...]	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 28. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
2	But if you include all the carve-outs, and we know the carve-outs to be significant—we know the carve-outs of the whitelisted apps and of API access to be significant […]. There were all these carvets [Sic], so the question is, do the exceptions swallow the rule?	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4333, Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.
3	There is also confusion there. In the whitelisted apps story that The New York Times ran in June, the story about Blackberry, in that case those apps would, for example, have access to friends' information. I actually tweeted a screenshot […]	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4335, Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.

4	All whitelisted companies used a standard form agreement called a »Private Extended API Addendum«, […]	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 122-123. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
5	This architecture means that if a bad actor gets a hold of these tokens, such as in the case of Pinterest, there is very little the user can do to prevent their information from being accessed. Facebook prioritises these developers over their users.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4327, Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.
5	[...] Remember the Facebook hack last week that compromised at least 50m accounts? It's worse than you think. Last Friday, the social media company revealed a vulnerability that allowed attackers to steal automated log-in credentials (or "tokens"). The tokens make it easier for people to log into popular apps and services like Spotify, Pinterest or Yelp. The flaw, which has been present since July 2017, was discovered last month after Facebook engineers noticed unusual login activity. [...]	Tynan, D. (2019, 14. Mai). Huge Facebook breach leaves thousands of other apps vulnerable. The Guardian. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens
6	The FTC had found that Facebook misrepresented its claims regarding their app oversight programme, specifically the »verified apps programme«, which was a review allegedly designed to give users additional assurances and help them identify trustworthy applications. The review was non-existent and there was no oversight of those apps.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 29. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
6	[…] before it awarded the Verified Apps badge, Facebook took no steps to verify either the security of a Verified Application's website or the security the Application provided for the user information it collected, beyond such steps as it may have taken regarding any other Platform Application.	US Federal Trade Commission. (2012, Juli). In the Matter of Facebook Inc., a corporation: Complaint (C–4365), S. 15. https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf
7	It was always kind of shady that Facebook let you volunteer your friends' status updates, check-ins, location, interests and more to third-party apps. While this let developers build powerful, personalized products, the privacy concerns led Facebook to announce at F8 2014 that it would shut down the Friends data API in a year. Now that time has come, with the forced migration to Graph API v2.0 […]	Constine, J. (2015, 28. April). Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps. TechCrunch. https://techcrunch.com/2015/04/28/facebook-api-shut-down/
7	There was a grace period of, I think, a year in which they allowed that setting, and then they also gave certain apps a small grace period. Then they allowed whitelisted apps to completely override that setting altogether.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4342 Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.

7	Old apps were given a year to continue to operate under the old rules. Facebook basically said that there were two versions of the API: the orginal and the new version. The old version, which run for another year, was allowed to operate as before.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Dr. Alexandr Kogan (Nr. HC 363). House of Commons, Q2041.
8	Facebook, updated the API to version v2.x (April 2014), and replaced the friends_xxx permissions with the single user friends permission, claiming that since 2015 (API v2.0) this problem has been mitigated; it required mutual consent and mandated app reviews. However, in our previous work we could retrieve information of arbitrary friends up until the API v2.3 (April 2014 - July 2017) using the Graph API interface. In der Fußnote ist zu lesen: We contacted Facebook to report the discrepancy between the stated mutual acceptance of an app for the information collection and the results we retrieved from the Graph API (v2.0 - v2.3). However, we received no response up to now (April 2018).	Symeonidis Et Al. (2018). Collateral damage of Facebook third-party applications: a comprehensive study, S. 2. https://eprint.iacr.org/2018/285.pdf.
9	Coming from Facebook itself, v2.x of the API has the potential to decrease both the likelihood and the impact of collateral information collection. […] Third, this API change does not have any effect on multi-app data fusion.	Symeonidis Et Al. (2018). Collateral damage of Facebook third-party applications: a comprehensive study, S. 2. https://eprint.iacr.org/2018/285.pdf.
9	For instance, the app providers VipoKomunikacijos and Telaxo offer 163 and 130 apps; among those, 99 and 118 have more than 10 000 monthly active users, respectively (extracted from the AppInspect dataset). As a consequence, an app provider may cluster several apps and thus may collect more personal data from the profile oftheusers.	Symeonidis Et Al. (2018). Collateral damage of Facebook third-party applications: a comprehensive study, S. 2. https://eprint.iacr.org/2018/285.pdf.
10	[…] making an app on Facebook […]. You don‘t talk to an human being. There is no contract you engage in. You go to an portal and say I want develop an app […]	Senate Commerce, Science,and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. (2018, Juni). Cambridge Analytica and Facebook Data Partners. Witness: Dr. Alexandr Kogan. C-Span. https://www.c-span.org/video/?447132-1/senate-committee-examines-cambridge-analytica-partnership-facebook
10	[…] I don‘t think they have a developer policy that is valid. […] For you to break a policy it has to exist and really be there policy. The reality is that Facebook‘s policy is unlikely to be there policy.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Dr. Alexandr Kogan (Nr. HC 363). House of Commons, Q1188.

10	Facebook not only left gaps in its privacy policies but also enforced those policies unevenly depending on how much revenue third parties were generating for the company. Internal documents noted that Facebook would allow apps spending more than a certain threshold on advertising to collect excessive user information, while Facebook would terminate access to apps spending less than that threshold. This selective enforcement and other related conduct were clear violations of the order.	US Federal Trade Commission (FTC) & Chopra, R. (2019, Juli). Dissenting Statement of Commissioner Rohit Chopra: In re Facebook, Inc. (Nr. 1823109). https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf
10	[…] There were only a handful of law suits and bans. Those were both quite rare. Mostly what I did was to call developers and threaten to do other things, basically saying that they needed to follow the policies. That was effectively the main enforcing mechanism during my time.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1966.
10 & 11	In addition, the complaint alleges that Facebook improperly policed app developers on its platform. The FTC alleges that, as a general practice, Facebook did not screen the developers or their apps before granting them access to vast amounts of user data. Instead, Facebook allegedly only required developers to agree to Facebook's policies and terms when they registered their app with the Facebook Platform. The company claimed to rely on administering consequences for policy violations that subsequently came to its attention after developers had already received data about Facebook users. The complaint alleges, however, that Facebook did not enforce such policies consistently and often based enforcement of its policies on whether Facebook benefited financially from its arrangements with the developer, and that this practice violated the 2012 order's requirement to maintain a reasonable privacy program.	FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions. (2020, 28. April). Federal Trade Commission (FTC). https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
11	Was there misuse of Facebook Platform? There may well have been. However, Facebook did not investigate deeply enough to determine exactly whether misuse took place.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1224.

11	[…], but the impression that I got was that if Facebook did an investigation and received information that showed that policies were being broken and potentially laws were being broken, then Facebook was liable. However, if Facebook did not know what was happening, they could claim that they did not know, they were simply a platform and what third parties do on their platform is not something that youc ould sue Facebook for.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1228.
11	In fact, Facebook confirmed that it never reviewed the TYDL App’s privacy policy. Facebook also confirmed that it never reviewed whether the TYDL App adequately sought consent to access Installing Users’ personal information. Facebook argued that given the volume of apps on its platform, it would be »too costly« to review privacy policies of third-party apps, or to ensure that those apps adequately described how users’ information obtained from Facebook	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002), RN63. https://www.priv.gc.ca/en/opc actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
11	**Facebook had inadequate safeguards to protect user information.** Facebook relied on contractual terms with apps to protect against unauthorized access to users’ information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
11 & 15	The other thing to note is that Facebook had relatively low detection of policy violations […]	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1188.
12	[…] you were involved in a few cases of action being taken against developers for breaching Facebook‘s terms for using data. […] were Facebook users notified […]? No, not tomyknowledge.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1200.
13	I am not aware of any breach notice that we had received, particularly from a technology company, but not from Facebook. […]	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Elizabeth Denham, Information Commissioner. (Nr. HC 363). House of Commons, Q4276.

14	I asked Facebook this morning about their business model. I have concerns about the way that app developers seem to be sharing information with Facebook, almost as a matter of course. I asked for a single example of a case where Facebook had withdrawn services to a business because of a breach, and they could not provide me with one.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Elizabeth Denham, Information Commissioner. (Nr. HC 363). House of Commons, Q4279.
15	There was concern inside Facebook then that other developers were building their own social networks because they had accessed so much friend data that they could see most of the social graph of Facebook.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1230.
15	With respect to monitoring, we recognize that Facebook pro-actively reviewed the top 500 apps on a regular basis, used certain automated criteria to flag potential apps for manual review, and had the ability to investigate apps that were reported by users or the media. However, in our view, these were, and remain, ineffective measures for monitoring the other tens of millions of apps and third-parties using the Platform.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002), RN156. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
15	Facebook’s automated tools were also insufficient to protect user information from being used in ways that ran counter to Facebook’s Platform Policy **prior to any misuse**. Before App Review was implemented, Facebook did not proactively monitor whether apps were requesting permissions and planning to use information in line with the Platform Policy before Facebook disclosed information to those apps. Only **after** App Review was implemented, did Facebook begin looking at apps’ permissions requests *before* disclosing information to those apps.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002), RN159. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
15 & 16 & 18 & 19 & 20	In November 2011, the US Federal Trade Commission (FTC) made a complaint against Facebook on the basis that Facebook had, from May 2007 to July 2010, allowed external app developers unrestricted access information about Facebook users’ personal profile and related information, despite the fact that Facebook had informed users that platform apps »will access only the profile information these applications need to operate«.	Digital, Culture, Media and Sport Committee Disinformation and »fake news«: Final Report / HC 1791 Published on 18 February 2019 by authority of the House of Common S. 23 RN 66 / USA Trade Federal Commission, in the matter of Facebook Inc, DOCKET NO. C-4365, July 2012, S. 10 / RN 30

15 & 19 & 20	[…] in many instances, a Platform Application could access profile information that was unrelated to the Application’s purpose or unnecessary to its operation. For example, a Platform Application with a narrow purpose, such as a quiz regarding a television show, in many instances could access a user’s Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook’s web site, despite the lack of relevance of this information to the Application.	US Federal Trade Commission. (2012, Juli). In the Matter of Facebook Inc., a corporation: Complaint (C–4365), S. 10. https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf
15 & 16 & 17 & 19	Facebook has represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as “Only Friends” or “Friends of Friends.” In truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as »Only Friends« or »Friends of Friends« through their Profile Privacy Settings. Instead, such information could be accessed by Platform Applications that their Friends used.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 25-26. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
16 & 17 & 21	In short, I found that time and time again Facebook allows developers to access personal information of users and their friends, in contrast to their privacy settings and their policy statements.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Ashkan Soltani, tech expert (Nr. HC 363). House of Commons, Q4327, Video der Aussage https://www.youtube.com/watch?v=kK1ZajDW-es.
16 & 17	Some preinstalled apps were able to circumvent users’ privacy settings or platform settings, and to access friends’ information as well as users’ information, such as birthdays and political affiliation, even when the user disabled the platform.	Digital, Culture, Media and Sport Committee Disinformation and »fake news«: Final Report / HC 1791 Published on 18 February 2019 by authority of the House of Common S. 29 RN 88House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 29. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
16 & 19	As set forth in Paragraph 30, Facebook has represented, expressly or by implication, that it has provided each Platform Application access only to such user profile information as the Application has needed to operate. In truth and in fact, as described in Paragraph 31, from approximately May 2007 until July 2010, in many instances, Facebook has provided Platform Applications unrestricted access to user profile information that such Applications have not needed to operate. Therefore, the representation set forth in Paragraph 32 constitutes a false or misleading representation.	US Federal Trade Commission. (2012, Juli). In the Matter of Facebook Inc., a corporation: Complaint (C–4365), S. 10. https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf

17	[…] when the Cambridge Analytica data scandalwas revealed and the vast majority of Facebook users had no idea that their data was able to be accessed by developers unknown to them, despite the fact that they had set privacy settings, specifically disallowing the practice.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 25. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
18	Siehe diverse Publikationen zu Facebook's Permission-System.	Na Wang et al. (2011). Third-party apps on Facebook: Privacy and the illusion of control. https://doi.org/10.1145/2076444.2076448. www.researchgate.net/publication/239761048_Third-party_apps_on_Facebook_Privacy_and_the_illusion_of_control
		Symeonidis et al. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. https://eprint.iacr.org/2018/285.pdf
		Symeonidi et al. (2015). Collateral damage of Facebook Apps: an enhanced privacy scoring model. https://eprint.iacr.org/2015/456.pdf
18	**Facebook failed to obtain valid and meaningful consent of installing users.** Facebook relied on apps to obtain consent from users for its disclosures to those apps, but Facebook was unable to demonstrate that: (a) the [...] App actually obtained meaningful consent for its purposes, including potentially, political purposes; or (b) Facebook made reasonable efforts, in particular by reviewing privacy communications, to ensure that the [...] App, and apps in general, were obtaining meaningful consent from users.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
18 & 21	Facebook's Graph API (v.1) allowed developers to collect Facebook profile data from users who directly installed or otherwise interacted with the developer's application or website through a Facebook Login (»App Users«), as well as from these users' Facebook »friends.« Facebook allowed this data collection even though the »friends« did not have any direct interaction with the app or website (»Affected Friends«).	United States Federal Trade Commission (FTC). (2019). In Matter Cambridge Analytica, LLC, a corporation: Opinion of the Commission (Nr. 9383), S. 3. https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf

19	As data is used for other purposes than the ones stated at the time of its collection, it may lose its contextualintegrity. […] A player that demonstrates a powerful way for the decontextualization is Facebook. Facebook encourages ist users to provide information as accurate, real, valid and complete as possible […]. Facebook is not known for directly selling the personal profiles […]. However, the company allows a large group of marketers and developers to leverage user data for […] other purposes. […] how Facebook has created an »asymmetrie« between the user‘s imagined and actual audience […].	Christl, W. & Spiekermann, S. (2016). Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. facultas, S. 121.
19	As a result, Affected Users for any app, including the TYDL App, had no way of truly knowing what personal information would be disclosed to which app and for what purposes. [...] We do not find it reasonable to expect users to provide consent, in advance, to disclosures of their personal information that could occur years later, to unknown apps for unknown purposes.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002), RN102. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
19	I think the problem is that Facebook users may have understood in theory that there were privacy concerns but they did not know how much of their data was being sent to developers whom they had no realtionship with.	House of Commons Digital, Culture, Media and Sport Committe. (2018, März). Oral Evidence: Fake News. Witness: Sandy Parakilas, former Facebook operations manager (Nr. HC 363). House of Commons, Q1197.
19 & 21	We fined Facebook because it allowed applications and application developers to harvest the personal information of its customers who had not given their informed consent—think of friends, and friends of friends— and then Facebook failed to keep the information safe. […] It is not a case of no harm, no foul. Companies are responsible for proactively protecting personal information and that’s been the case in the UK for thirty years. […] Facebook broke data protection law, and it is disingenuous for Facebook to compare that to email forwarding, because that is not what it is about; it is about the release of users’ profile information without their knowledge and consent.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 21. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
21	Facebook entered into »whitelisting agreements« with certain companies, which meant that, after the platform changes in 2014/15, those companies maintained full access to friends’ data. It is not fully clear that there was any user consent for this, nor precisely how Facebook decided which companies should be whitelisted or not.	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 27. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

21	[…] and also refers to »pulling non-app friends out of friends.get«, thereby prioritising developer access to data from users who had not granted data permission to the developer […]	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 33. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
21	**Facebook also failed to obtain meaningful consent from friends of installing users.** Facebook relied on overbroad and conflicting language in its privacy communications that was clearly insufficient to support meaningful consent. [...] Facebook further relied, unreasonably, on installing users to provide consent on behalf of each of their friends, often counting in the hundreds, to release those friends' information to an app, even though the friends would have had no knowledge of that disclosure.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
22	In 2009, the OPC concluded an investigation into Facebook, examining [...], disclosures to third-party applications on the Platform. [...] OPC recommended that Facebook implement measures [...]: a. To limit application developers' access to user information not required to run a specific application; b. Whereby users would in each instance be informed of the specific information that an application requires and for what purpose; c. Whereby users' express consent to the developer's access to the specific information would be sought in each instance; and d. To prohibit all disclosures of personal information of users who are not themselves adding an application. [...] Facebook declined to implement these measures. The final report concluded that Facebook: (i) failed to obtain meaningful consent from its users—including app users' friends—to disclose their information; and (ii) had inadequate safeguards in place to monitor compliance by app developers with Facebook policies.	Office of the Privacy Commissioner of Canada. (2019). Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia (Nr. 2019–002). https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/
22	On 27 October 2012, Mark Zuckerberg sent an internal email to Sam Lessin, […] that he was sceptical about the risk of such data leaking from developer to developer, which is, of course, exactly what happened during the Cambridge Analytica scandal. »[…] 'I'm generally sceptical that there is as much data leak strategic risk as you think. I agree there is clear risk on the advertiser side, but I haven't figured out how that connects to the rest of the platform. I think we leak info to developers, but I just can't think if any instances where that data has leaked from developer to developer and caused a real issue for us. Do you have examples of this?«	House of Commons Digital, Culture, Media and Sport Committee. (2019, Februar). Disinformation and »fake news«: Final Report (Nr. HC 1791). House of Commons, S. 32-33. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf