English Translation of German Original

PFR RECHTSANWÄLTE

Handelsgericht Wien
Marxergasse 1a
1030 Wien

Schriftsatz im webERV eingebracht

Wien, am 31.07.2014
SchreMa/facebook/wp//
V:\fb Beilagen\final_kons.docx

Klagende Parteien: **Mag. Maximilian Schrems,** geb. am 1. Oktober 1987,
Doktorand
[redacted]

vertreten durch: Proksch & Fritzsche Frank Fletzberger
Rechtsanwälte GmbH
Tel. 01/877 04 54
Nibelungengasse 11
1010 Wien
Code P111395

Vollmacht gem. § 8 RAO erteilt

Beklagte Partei: **Facebook Ireland Limited**
Reg. Nr. 462932 im Unternehmensregister der Republik Irland
Hanover Reach, 5-7 Hanover Quay,
Dublin 2 Ireland

wegen:	Feststellung und Unterlassung	€ 31.000,--
	Auskunft	€ 1.000,--
	Rechnungslegung	€ 4.000,--
	Leistung	€ 4.000,--
	gesamt	**€ 40.000,-- s.A.**

K L A G E
2-fach / Beilagen ./A bis ./AC

I. The Parties

1. Defendant is a company incorporated in the Republic of Ireland with its registered office in Dublin and a subsidiary of the US-American company *Facebook Inc*. having its registered office in Menlo Park, California, USA.

2. While Defendant's parent company (*Facebook Inc*.) serves the U.S. and Canadian markets, Defendant is responsible for operating the social network *facebook.com* and the www.facebook.com portal which was set up for that purpose on a worldwide scale outside of the two stated countries. This is also in keeping with provisions of section 19.1 of Defendant's Statement of Rights and Responsibilities of 15 November 2013 (Enclosure ./A) according to which Defendant is the contracting party of all users outside of the U.S.A. and Canada.

3. Given its worldwide scope of operations, Defendant does not only accept registrations from Austria, but operates – inter alia – also a specific local website in and for Austria; it owns the corresponding domain (URL: www.facebook.at, cf. WHOIS register extract, Enclosure ./B) and is engaged in further business activities (e.g. cooperations with Austrian companies, specific advertising for local users etc.) in Austria. Within the meaning of Article 15(1) point (b) [TN1] of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Defendant therefore directly targets its commercial activities also to Austria.

4. Since 8 June 2008 Plaintiff has been a user of the services offered by Defendant and hence a contracting partner of Defendant. Plaintiff is an Austrian citizen and consumer within the terms of section 1 *KSchG* (Consumer Protection Act), Article 5 Rome Convention on the law applicable to contractual obligations (Federal Law Gazette BGBl III No 166/1998, as amended by BGBl III No 84/2007), Article 6 of Regulation 593/2008/EC ("Rome I Regulation") and Article 15 of Council Regulation (EC) No 44/2001. Plaintiff has his habitual residence and domicile in Vienna.

Evidence: Examination of the parties

Statement of Rights and Responsibilities of 15 November 2013, Enclosure ./A

WHOIS entry for the URL facebook.at, Enclosure ./B

If contested, submission of further documents.

II. The Facts / Wrongful Behaviour of Defendant

A. General

Defendant's service (*facebook.com*)

5. As mentioned, Defendant operates the social network *facebook.com* worldwide outside the U.S.A. and Canada. This network allows users to upload various contents (e.g. texts, photos, videos, events, posts or personal information) and share them with other users depending on the chosen settings. These contents may also be enriched by other users (e.g. by adding comments, "likes" or tags in photos or other contents).

6. At first glance, Defendant's services do not differ essentially from other so-called "hosting" services (web server, YouTube, WordPress installations), which allow users to place contents (photos, videos, blogs, websites) on the internet.

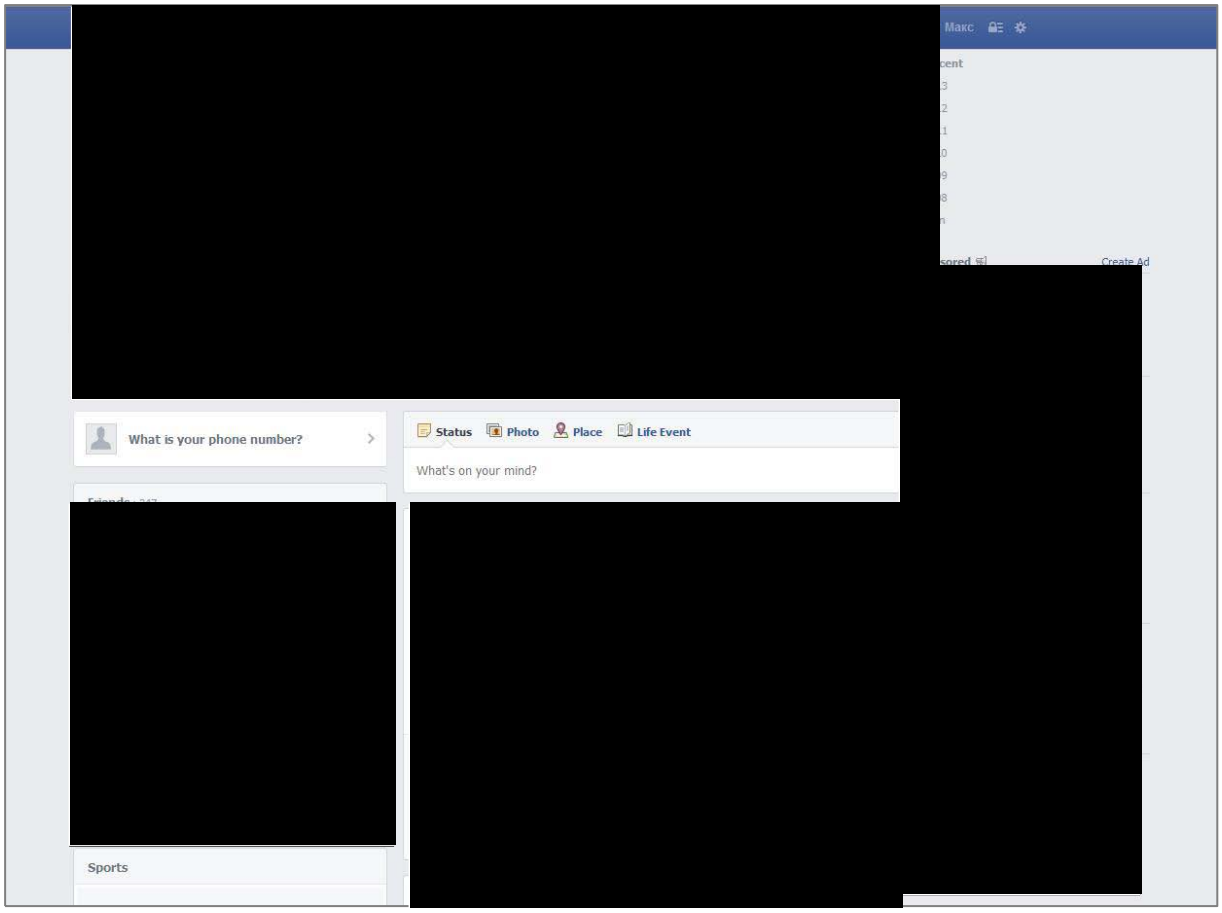

Fig. 1: Plaintiff's page (Timeline) on facebook.com

7. The users of Defendant's services may also communicate directly with other users and "chat" with them as well as share data via direct messages and emails. These services of Defendant equally do not differ from those of comparable communication services.

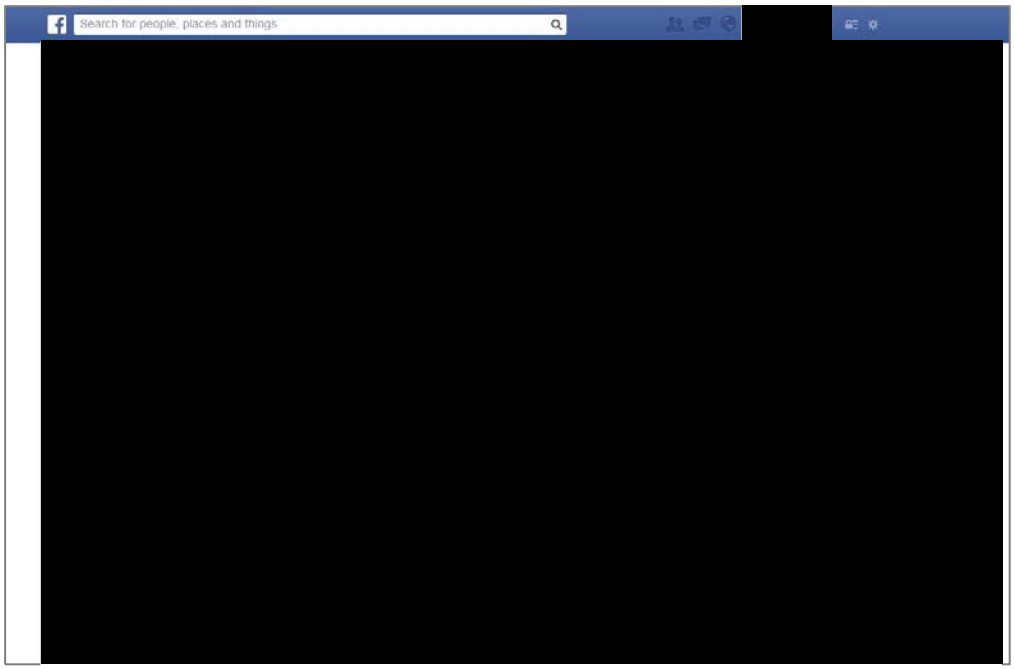

Fig. 2: Plaintiff's messages on facebook.com

8. In addition to the above features (offered by many other online services as well), every user may add other users as "friends". These "friends" usually run into extremely high numbers (500 or even 1000 "friends" are not uncommon) and would therefore rather qualify as "loose acquaintances" in common parlance. It is also quite common that users do not know all their "friends" in person or have forgotten who they really are. The "Friends" function is a key feature with sets this service of Defendant apart from other services.

Fig. 3: Plaintiff's friends on facebook.com

9. Many of the features provided by Defendant interact strongly with the individual user's "friends" network. Through the "friends", the user's social environment and his communications within this network are recorded. In this manner, virtually all information of all users is linked. This linking of innumerable data with the users is called "social graph" by Defendant and allows analysing information beyond individual users and the data they themselves provide. It is such possible to extrapolate information about the user which he himself did not furnish from e.g. information on the user's environment.

Defendant's business model

10. Defendant does not generate contents itself but receives these contents from private and commercial users like Plaintiff (see Fig. 4 below) for its services without a direct compensation of costs and/or without paying any set "consideration". Defendant limits itself to providing and administering the infrastructure and offering features for automatic aggregation of user data.

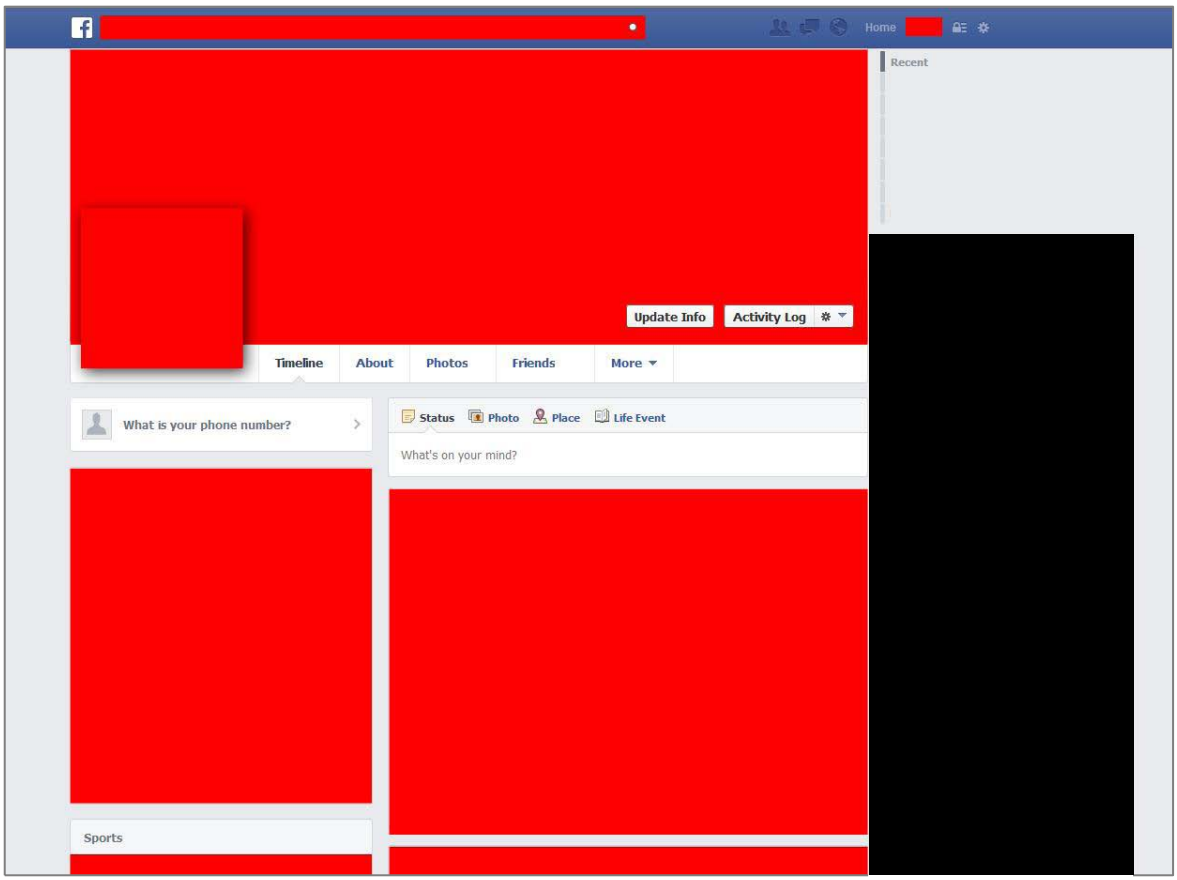

Fig. 4: User page without user contents (red) and with advertisements (framed in green)

11. This business model is called 'Web 2.0' and describes the shift of content generation from an Internet site operator to the user ("user-generated contents"). The commercial advantage over "classic" internet sites consists in the fact that contents are obtained at no direct own (e.g. production or editing) costs. The contents such obtained are to stimulate a maximum use of the website ("traffic") which in turn is crucial for placing advertising.

12. This is also reflected in Defendant's Statement of Rights and Responsibilities (Enclosure ./A) which provides, inter alia, in section 2.1 that *facebook.com* users grant their intellectual property rights in the uploaded contents to Defendant. In section 10.1 of the Statement of Rights and Responsibilities, Defendant even stipulates that the name and the photos of users may be used for third-party advertising ("Max Schrems likes company X").

13. Consequently, the Statement of Rights and Responsibilities must be considered as a framework agreement. The individual transaction is perfected by the act of uploading, which triggers a transfer of the rights of use – as well as Defendant's hosting service. Given the exchange of services of a pecuniary value, the contract between Defendant and its users must in this respect at any rate be considered as "against payment". This business model is also common to other Web 2.0 services.

14. According to its own information, Defendant makes its profits primarily through advertising which is placed in highly different forms in Defendant's services. Companies may also support their contents financially ("sponsoring") and thereby ensure that these contents are shown to a larger number of users. In addition to relatively static advertising (displayed to all users equally), Defendant also offers various "customized" forms of advertising which allows advertisers to specifically target individual groups of persons (e.g. by place, age, sex, interests – see Fig. 5 below) and even individuals (e.g. in customer "re-targeting").

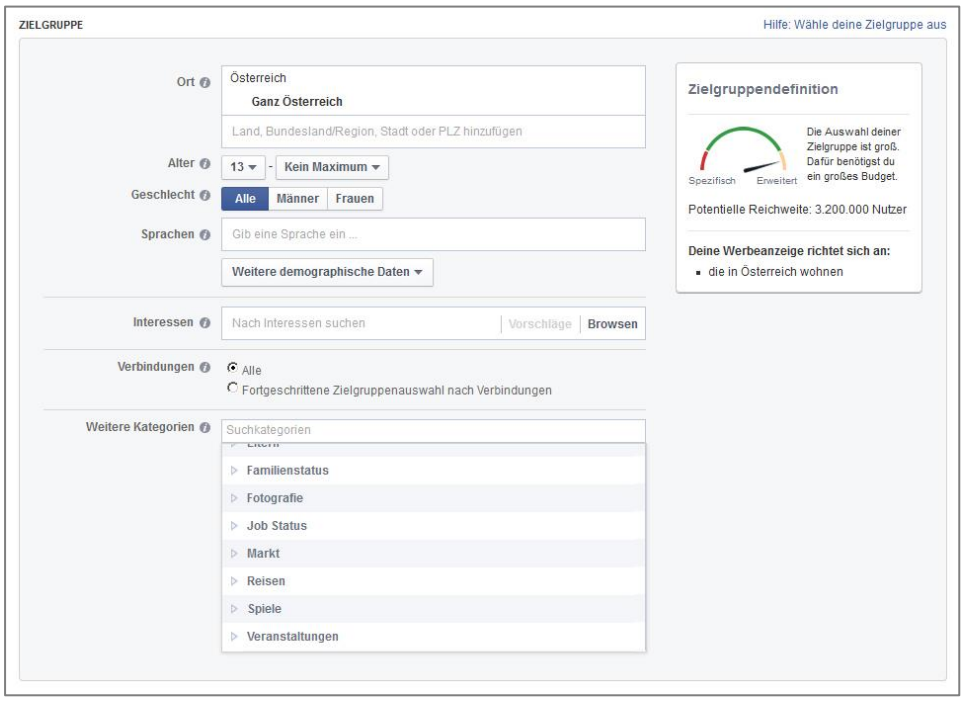

Fig. 5: Most simple form of target group selection for advertisers on facebook.com

15. To this end, Defendant analyses the data available on every user and tries to explore users' interests, preferences and circumstances. The exploration of user 'likes' or 'profiles' is not only based on the interests or information furnished by the user himself, but on all personal data available to Defendant, including in particular user data provided by third parties, results from the interlinking of data, and user information collected independently by Defendant. The precise systematics on which these analyses are based is not disclosed by Defendant.

Defendant's monopoly

16. Defendant is estimated to have approx. 3.2 million active users in Austria (worldwide, this number is purported to have already reached approx. one billion). With somewhat less than 6 million internet users older than 14 in Austria, this constitutes more than 50% of all Austrian internet users. By comparison, the factually biggest competitor ("Twitter") is estimated to have only 50,000 to 60,000 active users and such a market share of less than 1% in Austria.

17. Defendant's market clout is not only rooted in the free choice of users: Since Defendant offers a "closed" communication network, a change of provider is virtually impossible for users. While consumers may register with alternative networks (such as e.g. "Google+"), they cannot communicate from there with their "friends" on *facebook.com* and can therefore only be "socially alone" with alternative providers, which prevents a dynamic exchange. Graphically speaking, this compares to a situation where it would be impossible to maintain contacts between different email providers or mobile phone networks: Users changing to an alternative provider would be isolated. Even large-scale alternatives have not been able to assert themselves vis-à-vis the service operated by Defendant.

18. Concurrently, the social network has become a standard form of communication (similar to email, telephone or text messaging) for an overwhelming part of the population. Summarizing, Defendant enjoys a de-facto monopoly of a meanwhile widely used and/or common communication service in Austria as well as on most markets around the globe (with some exceptions such as China or Russia).

Legal classification of data

19. For the sake of further argument it appears expedient to legally classify the data which are provided by users and processed by Defendant. Under Austrian law, such data are considered a property within the meaning of section 285 *ABGB* (General Civil Code), in which ownership can be created (according to the "wider notion of property" set out in the *ABGB*). Other legal systems provide for a similar economic classification of data, otherwise e.g. the sale of customer files, electronic databases or similar would not be possible. As with other forms of ownership, rights may be limited or shared by several persons.

20. Irrespective of ownership in data, other rights (e.g. copyrights) may exist in the same data and limit ownership. Ultimately, general rights to the protection of personality may be connected to such data. This manifests itself in particular in the right to data protection, if the data concern an identified or identifiable person.

B. Distribution of roles in data protection law

21. Harmonised by European legal provisions, the data protection laws of Austria and Ireland provide for a clear distribution of roles, based on

- *Betroffener*/data subject, whose personal data are being processed (within the meaning of section 4 para 3 *DSG*, Austrian Data Protection Act, corresponding to the "*data subject*" of Article 2(a) of directive 95/46/EC and the "*data subject*" in s 1(1) of the Irish Data Protection (DPA), hereinafter "data subject"),
- *Auftraggeber*/data controller (within the meaning of section 4 para 4 *DSG*, *Austrian Data Protection Act,* corresponding to the "controller" of Art 2(d) of directive 95/46/EC and the *"data controller*" in s 1(1) DPA, hereinafter "controller"), and
- one or several *Dienstleister*/data processors as appropriate (within the meaning of section 4 para 5 *DSG*, Austrian Data Protection Act, corresponding to the "*processor*" in Art 2(e) of directive 95/46/EC and the "*data processor*" in s 1(1) DPA, hereinafter "processor".

22. Only data subjects are easy to identify, also with complex systems, since it can be readily assessed whether a person is "identified or identifiable" by given data.

23. Generally, the distribution of roles between data controller (operating company) and processor (hosting company) is clear, if processing is simply "outsourced" (e.g. where computers are being provided, so-called "hosting"). In all other cases, the distribution of roles must be assessed on a case-by-case basis, depending on the facts (also e.g. the Article 29 group in WP 169, p. 11, cf. also DSK in K121.533/007-DSK/2009).

The user as controller of his Facebook profile (first part of processing)

24. In general, users can freely dispose of their Facebook page, their posts, photographs etc. They create, edit and delete these data. They choose *facebook.com* as a system and processor and can theoretically end this processing of data.

25. Hence, Plaintiff and all other users are controllers within the meaning of section 4 para 4 *DSG,* Austrian Data Protection Act) (which apparently is also assumed by *Article-29-Group* in WP 163, pages 6 and 7) for the purposes they pursue (e.g. self-presentation, communication or administration of contacts). As regards these purposes, Defendant is only a processor.

26. Even being a "private user" does not alter Plaintiff's classification as controller, since a public website (a user's Facebook profile in its standard setting is nothing but such a public website)

falls outside of the scope of a "purely personal or household activity" within the meaning of Article 3(2) of directive 95/44/EC [TN2], for its mere wording alone, and also following a clear decision of the CJEU in C-101/01 *Lindqvist.*

27. Furthermore, the Austrian Data Protection Act (to which Plaintiff is subject) does not grant a general exemption concerning private users, but provides for simplifications to a limited extent (see e.g. section 17 para 2 subpara 4 and section 45 *DSG,* Austrian Data Protection Act). What is more, the transfer from the user's private sphere to a commercial controller such as Defendant no longer qualifies as a "purely private or household activity".

28. Ultimately, the definitions and role distributions of the *DSG,* Austrian Data Protection Act, must be retained also with private users privileged under Article 2(2) directive 95/46/EC, or else a legal void would be created. Data processing without a controller would e.g. not entail any obligations for the data processor.

29. Inasmuch as the user processes his own data (own photos, posts, videos), he is data subject and controller in one person. If, however, he also processes the data of other subjects (e.g. by uploading a photograph of several persons, importing contact data or commenting on a third party), he becomes a controller who processes personal data of other data subjects.

Defendant as controller of further data processing operations (second part of processing)

30. In addition to its role as processor of user data, Defendant further processes and uses the data provided by users also for its own purposes, which are not known and not disclosed to the individual users and/or controllers: i.e. by conducting statistical analyses of the preferences of all data subjects for the purpose of selling advertising services to third parties, analysis of data for its own advertising, data aggregation (e.g. for the "Newsfeed") and similar. Defendant does not allow the user to intervene in the processing of the data and does not even inform him about the precise steps of processing for those other purposes. By processing these data independently, Defendant transcends its role as processor and becomes a controller itself (along the same lines see e.g. *Dohr/Pollierer/Weiss/Knyrim*, DSG^2, 14. Erg.-Lfg., § 4, note 6; *Jahnel*, Datenschutzrecht, 3/50 et seq.; *Peter Carey*, Data Protection, 11-16 et seq.;).

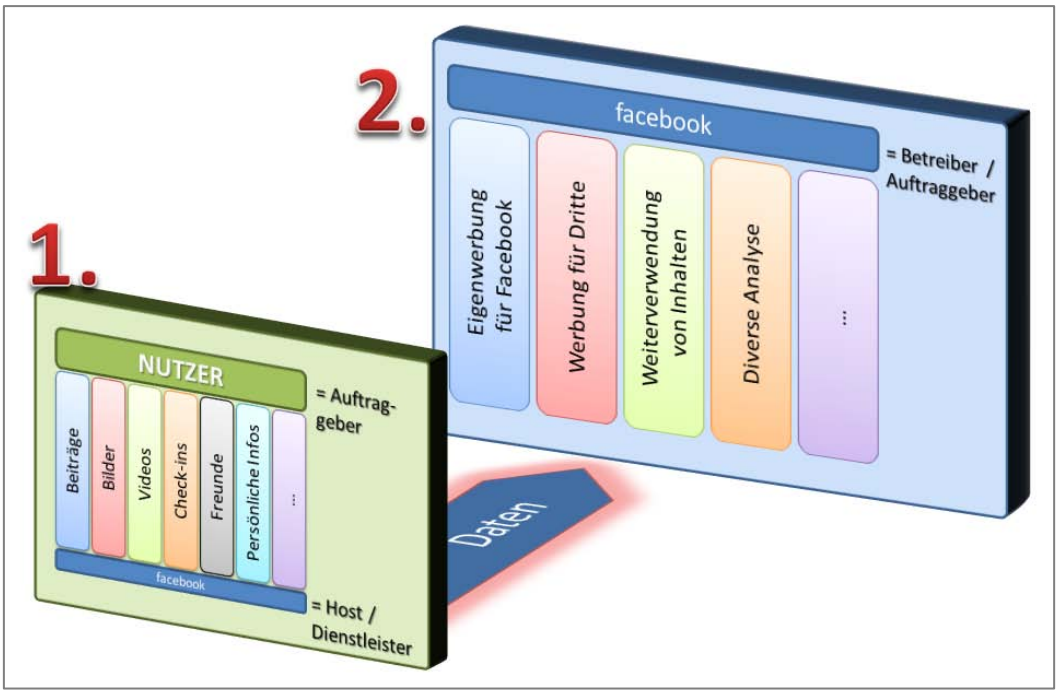

Fig. 6: Data processing by Plaintiff (1) and data processing by Defendant (2)

31. In legal terms, this further use by Defendant for other purposes constitutes a "transmission" within the meaning of section 4 para 12 *DSG*, Austrian Data Protection Act, from a controller (Plaintiff) to another controller (Defendant). Such transmission is admissible only at the conditions set out in section 7 para 2 *DSG* and in the general principles laid down in sections 6, 7 and 8 or 9 *DSG* (in conjunction with section 45 *DSG* as appropriate) (along these lines also e.g. *Jahnel*, Datenschutzrecht, margin number 8/8;). As will be elaborated in the following, Defendant is seriously and consistently breaching these obligations.

Legal duty to determine the distribution of roles

32. A duty to specifically determine the roles and the respective rights and obligations of controllers and processors can be derived from Article 6(2), Article 16 and Article 17(2) to (4) of directive 95/46/EC and accordingly from section 10 para 1 *DSG,* Austrian Data Protection Act, and s 2C(3) DPA.

Lack of clear determination by Defendant

33. Defendant offers its services exclusively after the acceptance of its Statement of Rights and Responsibilities (Enclosure ./A) and of its Data Use Policy (Enclosure ./C). Users do not have a possibility to add or negotiate different or other agreements. In order to be able to attribute the respective rights and obligations, the specific roles of the contracting parties as controller and processor would first have to be determined. Defendant's agreements do not lay down any clear-cut provisions on the distribution of roles under data protection law; on the contrary, Defendant's provisions contradict each other and become even less clear given a number of public statements made in this context.

34. In direct negotiations with Defendant on 6 February 2012, Richard Allen, a representative of Defendant, told Plaintiff: "*We are the controller for what we control... [and] ...the user has some responsibility too*" and such made clear that Defendant is unable to state a clear determination of roles. The corresponding meeting record is annexed as Enclosure ./D.

Evidence: As before

Defendant's Data Use Policy of 15 November 2013, Enclosure ./C

Extract from the meeting record of 6 February 2012, Enclosure ./D

35. In its Data Use Policy, Defendants states on the one hand under the heading "Information for users outside of the United States and Canada" (penultimate paragraph of the Data Use Policy) that it is "*the data controller*[1] *responsible for [the] personal information"* of the user; given the fact that the English version uses the term "controller" from Article 2(d) of directive 95/46/EC, this must indeed be understood as a statement by Defendant that it is the controller of all data processing operations. On the other hand, Defendant states in the same Data Use Policy: *"While you are allowing us to use the information we receive about you, you always own all of your information"*. Moreover, Defendant consistently speaks vis-à-vis the user of "your timeline", "your settings" and "control" of the user over "his" data, which according to common usage (at least as regards his Facebook page) suggests the user would be the controller.

36. In various public statements, Defendant has created the impression that the user is the controller responsible for his data, such as in a written interview in the German *"Stern TV"* news magazine (Enclosure ./E) in which a spokesperson of Defendant, Mr. Ardelt, clarified that the above provision is to be understood to mean that Defendant only "administers data" and that "data administrator" would be a more pertinent term to express its role as exclusively that of a processor.

37. In a public oral hearing on 5 December 2013 before the Austrian Constitutional Court, Dr. Gunnar Bender (representing Defendant) also took the position that Defendant was *not the controller responsible for the user pages*, but that these pages were supplied with content by the page owner (in this case the Austrian Broadcasting Corporation).

Evidence: Examination of the parties

As before

Written interview Stern TV, Enclosure ./E

Case file of the Constitutional Court, file no B 1035/2013-22 to be produced.

---

[1] Translator's note: the German version uses the term *Dateninhaber* for the term controller which would literally translate back as "data owner".

38. By contrast, Defendant maintained in a statement of 31 May 2013 (Enclosure .F) in proceedings before the administrative court of Schleswig-Holstein (case no 8 A 218/11) that it is *"sole controller for all pages and functions on facebook.com"* and denied that the page operators were controllers in any way. Apparently, this line of reasoning was intended for the German data protection authorities (which had issued injunctions against German users of *facebook.com*) to no longer be competent for those pages.

39. In other cases of illegal data featured on Facebook pages, Defendant denied any responsibility for user-provided data. In *McKeogh vs Facebook Ireland Limited et al.* (Irish High Court, Record No. 2012/254P, of 16 May 2013, para 14, Enclosure ./G) Defendant even held the view that it fell under the liability privileges of Articles 12 to 15 of directive 2000/31/EC for mere "conduit", "caching" or "hosting" (see also sections 13 to 19 *ECG,* Austrian E-Commerce Act) in cases where illegal data were processed on *facebook.com*. This line of reasoning was apparently intended to avoid an obligation to delete illegal contents in Ireland.

40. To summarize, the role distribution under data protection law for the different functions of *facebook.com* remains unclear to date. Defendant alters its legal view as it deems opportune: questions of liability or other problems are to be the sole responsibility of the user, while Defendant is only processor, "administrator" or "host"; when it comes to unrestricted processing and use of data, Defendant claims sole responsibility and controllership.

Alternatives to a "shared" distribution of roles

41. As an alternative to shared controllership depending on the purpose and/or processing operations, it would be possible for Defendant to have *sole* responsibility, which would imply however that Defendant specifically would have sole responsibility under the law for all uploaded data. Defendant would then, amongst others things, need the consent of data subjects who are not users of *facebook.com* whenever a user uploads data of those persons. Defendant would also have to ascertain and/or assess the legality of processing of every uploaded datum and would be liable for any unlawful statements (e.g. defamation, slander and libel, or National Socialist resurgence) which are disseminated by users via the *facebook.com* portal. Defendant is not likely to aim at such a scenario which, in addition, is inconsistent with how *facebook.com* currently works.

42. According to data protection law it is possible for several controllers to operate a data application *jointly* and to take decisions jointly. However, this situation does not apply here, since the users and Defendant process the data for different purposes and without any possibility of intervention. It is most likely not in Defendant's interest that the users have a say in decisions on advertising activities or similar data uses.

43. Both of these conceivable alternatives are unrealistic for the above reasons. In the following is it therefore assumed that the role of controller is divided and/or shared.

Evidence: Examination of the parties

As before

Defendant's Statement of 31 May 2013, Enclosure ./F

Extract from the judgment McKeogh vs. Facebook et al., Enclosure ./G

If contested, submission of further documents.

Submission of further evidence reserved.

C. Defendant's obligations as data processor

44. Pursuant to Directive 95/46/EC it is primarily the controller who must ensure that data are used and processed in conformity with the law. If he uses a processor for this purpose, the controller must ensure that the processor as well complies with the legal requirements and e.g. processes data only as ordered and conforming to the controller's instructions ("legitimate use of data" within the meaning of section 10 para 1 *DSG*, Austrian Data Protection Act). The European legislator pursues this objective in Article 16 and Article 17(2) to (4) of directive 95/46/EC which require a contract which binds the processor to the controller and his instructions.

45. Furthermore, a distinction must be made from the obligation to implement data security measures *("secure use of data"* within the meaning of section 10 para 1 *DSG,* Austrian Data Protection Act), which results directly from the law also vis-à-vis a processor (Article 17(3) second indent of directive 95/46/EC).

Defendant's "lawful use of data"

46. In section 11 *DSG*, the Austrian Data Protection Act adds direct statutory obligations of the processor to this contractual requirement. Irrespective of the fact that such statutory duties do not exist under Irish law, Plaintiff (as controller) must strive for a contractual relation with Defendant (as processor), given the legal requirement of section 10 para 1 *DSG,* Austrian Data Protection Act (and/or of Article 17(2) to (4) of directive 95/46/EC).

47. The Statement of Rights and Responsibilities (Enclosure ./A) and the Data Use Policy (Enclosure ./C) on which Defendant bases all its contracts are silent on any obligations of Defendant vis-à-vis the controller. Hence, the users of *facebook.com* are in a "contract-free" state which is not provided for in the directive and in the Austrian Data Protection Act. A claim to an agreement between Plaintiff and Defendant that is compliant with the law results *ex lege* from section 10 para 1 *DSG,* Austrian Data Protection Act (and/or Article 17(2) to (4) of directive 95/46/EC) and/or as an ancillary obligation to the existing contract between Plaintiff and Defendant, as

otherwise the services offered by Defendant for private and commercial users in Europe cannot be used in conformity with the law.

48. Add that Defendant currently does not, or only partially, comply with Plaintiff's instructions. After Plaintiff had requested Defendant several times to disclose the data it had processed, he was sent a CD in July 2011 with a pdf-file consisting of 1,222 pages in the print-out version. These data records created by Defendant contained a large number of data which Plaintiff had deleted earlier, but which Defendant had rendered merely "invisible" - a fact which Defendant had not disclosed to and/or had intentionally concealed from Plaintiff. Moreover, Defendant continued to use "deleted" friends to create profiles and to propose the friends of a "deleted" friend to users. Also, "deleted" tags in photos were set merely "invisible" by Defendant. As regards these cases, see by way of example Enclosure ./H.

Defendant's "secure use of data"

49. On data security (where the processor has a direct statutory obligation according to s 2(1)(d), 2(2) in conjunction with 2C(2) DPA and/or paragraph (3) [TN4] second indent of directive 95/46/EC), Defendant did make a statement, yet only in a manner that is not in conformity with the law: While section 3 of the Statement of Rights and Responsibilities reads: "*We do our best to keep Facebook safe, but we cannot guarantee it*.", this is followed by 12 points listing the user's (not Defendant's!) obligations. Along the same lines, the Statement of Rights and Responsibilities Enclosure ./A, reads under section 16.3: *"*WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS*".* The Data Use Policy, Enclosure ./C, contains a similar statement under the heading *"Some other things you need to know*" / subheading "Safety and bugs": "*We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services or products*."

50. Defendant's contractual provisions explicitly contradict Article 17(3), second indent of directive 95/46/EC and s 2(1)(d), 2(2) and 2C(2) DPA. In these points, users of *facebook.com* are exposed to an unlawful contractual state. A claim to a contractual agreement between Plaintiff and Defendant results from Article 17(2) to (4) of directive 95/46/EC and/or from section 10 *DSG,* Austrian Data Protection Act, and s 2(1)(d), 2(2) and 2C(2) DPA.

Evidence: As before

Extracts concerning non-"deleted" data, Enclosure ./H

If contested, submission of further documents.

Submission of further evidence reserved.

D. Consent of users under data protection regulations

The legal requirements for a valid consent

51. Article 7 or Article 8 of directive 95/46/EC generally prohibits any processing of data, unless the controller has given his explicit consent ("prohibition of reserved consent"). To start, it befits to recall that the burden of proof that data have been processed in conformity with the law rests with Defendant.

52. For those data applications for which Defendant is the controller, it invokes the "consent" (within the meaning of Article 2(h) of directive 95/46/EC, "*Zustimmung/consent*" pursuant to *DSG,* Austrian Data Protection Act) by the data subject to its Data Use Policy (Enclosure ./C).

53. In order to meet the requirement of consent set out in s 2A(1)(a) DPA (which corresponds to Article 7(a) and/or Article 8 point (a) [TN5] of directive 95/46/EC and to sections 8 and 9 *DSG*), the consent must be given "unambiguously", i.e. freely given, specific and informed. Since the Irish DPA, which is applicable to Defendant, does not provide for a definition of "*consent*", the definition in directive 95/46/EC is applicable in Ireland pursuant to s 1(3A) DPA (cf. also *Denis Kelleher*, Privacy and Data Protection Law in Ireland, margin number 11.06 et seq.).

54. The Irish legal situation conforms with directive 95/46/EC and corresponds to the transposition in the Austrian Data Protection Act; the DSG, however, does not refer to the notion of "unambiguously" (Article 7(a) of directive 95/46/EC) as compared to directive 95/46/EC but adds, by way of clarification, that the data subject can revoke his consent at any time (cf. section 8 para 1 subpara 2 *DSG*). This can, however, be directly inferred from directive 95/46/EC (also Article-29-Group in WP187, pages 16 and 39). Given full harmonisation, Austrian case law on consent (excepting the issue of revocation, as appropriate) is at any rate applicable to the present case.

55. The Data Use Policy, Enclosure ./C used by Defendant becomes a part of the contract upon the user's acceptance and by virtue of section 1 of the Statement of Rights and Responsibilities and doubtlessly qualify as "General Terms and Conditions" and/or contract forms. As regards Plaintiff and all Austrian users, if and when they are consumers, sections 864a, 879 para 3 and 915 *ABGB* (Austrian General Civil Code) as well as the transparency requirement of section 6 para 3 *KschG* (Austrian Consumer Protection Act) are applicable to Enclosure ./C under established case law. These provisions must be applied as overriding mandatory rules implementing directive 93/13/EEC on unfair terms in consumer contracts, irrespective of Defendant's choice of law, but at any rate also according to the laws of Ireland where Defendant has its registered office (cf. Irish transposition S.I. No 27/1995 as amended).

Case law on consent

56. In its established case law, the Austrian Supreme Court has developed the view that informed consent (Article 2(h) of directive 95/46/EC and/or section 4 para 14 *DSG,* Austrian Data Protection Act) can only be given if the specific data, the specific purpose and, as appropriate, the specific recipients of transmissions are conclusively and transparently indicated.

57. In 7 Ob 84/12x the Supreme Court held that the expression *"your master, traffic and other personal data"* together with a definition containing the words *"such as"* and "e.g." is intransparent, since a non-exhaustive enumeration of data does not achieve a limitation.

58. In the same case, the Supreme Court held that the clause "*for the purpose of providing added-value services, demand-oriented offers, producing demand analyses and to improve our products*" covered a such broad purpose that the customer was unable to form an idea as to what was going to happen with his data.

59. In 2 Ob 198/10x the Supreme Court held that the expression "to the extent this is necessary for obtaining information" and "to the extent necessary" within the framework of a transmission of data to third persons was totally indeterminate. This, it argued, would not allow for meaningful delineations, but would in actual fact make use of empty phrases.

60. In this case the Supreme Court also made it clear that only because a concrete delineation might be difficult would not justify depriving the data subject of his information rights.

61. On exchanges within "*group companies*" , the Supreme Court held in 2 Ob 1/09z (referring to 7 Ob 170/98w) that the data subject was unable to determine which companies presently and in the future belonged to the "group" (also abroad, as the case may be.) Therefore, a concrete designation of the recipients was lacking. The Supreme Court equally held that transmissions to *"associations for the protection of creditors"* and for the purpose of "*assessing financings and transacting payments*" was insufficiently concrete.

Defendant's Data Use Policy

Scope of the data protection regulations [TN6]

62. Defendant's Data Use Policy, Enclosure ./C covers 20 printed pages and consists of more than 10,500 words (including the table of contents and the "cookie" guideline). Practiced readers read a standard text at approx. 200 words per minute, unless it is extremely complicated. The resultant time required to read the entire document would therefore be 50 minutes, if one were to qualify it as a "standard" text. Since this is a legal text with at times convoluted sentence structures, the actual reading time is presumably significantly higher. Add the Statement of Rights and Responsibilities, Enclosure ./A with approx. 5,200 words. Considering the scope of its Data Use Policy and its terms and conditions alone, Defendant is overworking the "fiction of consent".

Structure of the Data Use Policy

63. Enclosure ./C is made up of 6 parts. However, one cannot immediately grasp a logical structure of the Data Use Policy used by Defendant. Part I seems to define the general rules on the use of data by Defendant as controller, Part II deals with data processing by the user, Part III with the interaction with third-party systems (e.g. "apps" and "platform" applications) in given cases, Part IV with advertising, and Parts V and VI with other issues.

64. Relevant information on every subject can also be found in other parts. It is unclear how the individual rules relate to one another, as Defendant uses e.g. a general clause which allows every (conceivable) use of data in the context of "developers" (presumably of "apps"), only to further describe this exchange of data in Part III of the Data Use Policy. For instance, it is completely unclear whether Part III is merely an explanation of the general clause, or whether it limits the latter as a special rule.

Use of language

65. In its Data Use Policy, Defendant consistently uses general clauses which are explained by vague, non-exhaustive and inconclusive examples. This use of language runs through all information on data sources, data types, purposes, use processes and transmission to third parties. In doing so, Defendant achieves that *de facto* any and every conceivable form of data use is covered linguistically by the wording of the provisions, without coming anywhere near to limiting their specific scope and purpose.

66. Moreover, Defendant often uses examples that contribute to playing down the general clauses. Of the many possible data uses within a general clause, the least problematic example is put first, for instance.

Collected data

67. The data sources and the data collected by Defendant are listed under the heading "Information we receive about you". This is introduced by the general clause "*We receive a number of different types of information about you, including:".* The following enumeration is such purely exemplary. The only legally relevant limitation of data acquisition by Defendant is "*a number of different types of information*", in other words a blanket authorisation to collect and use any form of data about the user.

68. The following non-exhaustive enumeration as well is beyond any measure of indeterminateness: Under "Your information", any and all data provided by the user or which are derived from interaction with the user are described as a general clause and explained by only very few non-exhaustive examples (e.g. log data, click data etc.). In this area as well, every click, every mouse movement and every bit which is generated in the interaction with Defendant, its services and data applications or with other users, would be covered by the statement. However, it is not stated which data specifically Defendant records and processes and for what purpose.

69. This is only topped by the section on "*Information others share about you*", which offers yet another general clause when stating: "*We receive information about you from your friends and others*" and is complemented only by "such as" and very scarce non-exhaustive examples.

70. Under "Other information we receive about you" further cases of direct data acquisition and transmission by third parties are mentioned. Again, one persistently finds phrases such as "sometimes", "for example" or "may", which show a high degree of vagueness. Defendant again makes it clear that all data whatsoever about the user, his friends and any "other" person may be linked and compiled to form new data ("big data"), so as to extrapolate and generate more information about the user than he himself has shared.

71. To summarize one must conclude that in its provisions Defendant does not limit the type of the collected data and the sources of these data in any way whatsoever, but grants itself the right to collect any type of data about the user from any source and even to create new personal data about the user (especially via aggregation and analysis).

Specified purpose of data use

72. Accordingly, under the heading *"How we use the information we receive"* one finds another general authorisation: *"We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use"*. This is followed by a list of examples of highly general data uses which Defendant grants itself "*additionally"*.

73. If one were to ask about the limitation to the processing of data achieved thereby, this statement excludes only such data uses which are not "*connected to the services and features"* of Defendant and which are not offered by Defendant to anyone. In a nutshell: Any conceivable use of data and everything that is merely connected to Defendant's services apparently is to be covered by the users' consent.

74. In the following paragraph, Defendant additionally grants itself the right "*to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways*." In this manner, Defendant could use all data at any time for any conceivable purpose and even purposes which are not even conceivable yet.

75. Summarizing, the Data Use Policy [TN7] does not give rise to any limitation of purpose. On the contrary, Defendant has a permission granted to itself for any form of data processing for any present or future purpose it may pursue.

Transmission of data to third parties

76. Under the heading "*How we use the information we receive"* there is a clause on the transmission of user data to third persons which clearly states that data must not be transmitted, unless we *"[1] received your permission; [2] given you notice, such as by telling you about it in this policy; or [3] removed your name and any other personally identifying information from it".*

77. While the last case would be unobjectionable (if correctly implemented technically and organisationally), it is sheer impossible for a consumer to keep an overview of when and how Defendant has received "permission" or has "given notice". In practical terms, this may happen in every corner and on every sub-page of the platform run by Defendant and also on third-party sites. The circle of potential recipients is neither limited, let alone is it made more concrete.

78. In its Data Use Policy, Defendant also furnishes the following information: "Information made "public" is publicly available, even if this information is made "public" by a third party without the user's permission".

79. Moreover it is stated that anyone and any of one's "friends" can transmit data to "apps" or via Defendant's API to third parties. Defendant shares user data with "partner third-party sites", with undisclosed "*service providers*", "*affiliates*" belonging to the same group of companies and with "other businesses" within the framework of cooperations. By the above general clause: "*We use the information we receive about you in connection with the services and features we provide to you and other users (...)*" transmission is covered also linguistically.

80. Defendant further states that it is allowed to share data in response to "*legal requests*", if it has "*a good faith belief that the law requires* [it] *to do so*", or if Defendant has "*a good faith belief*" that the response is required by law in that jurisdiction (not however the law of the jurisdiction in which Defendant has its registered office).

81. Defendant also assumes the right to share personal data if this is *"required to detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations."*

82. Summarizing, Defendant provides for a limited transmission, but then makes the user grant it a very wide and vague consent to transmission, and – on top of that – uses a "fiction of consent" by "information". The information provided is non-transparent, unspecific and not readily graspable for a consumer. It is in stark contradiction with relevant European and national data protection regulations.

83. The apparent reason for this comprehensive and systematic disregard of data protection law is Defendant's policy and/or approach: Seemingly, Defendant simply uses the information of its parent company (which is oriented on the minimal requirements of sections 22575 to 22579 of the California Business and Professions Code) in an identical wording as a basis for consent according to European law.

84. It follows that Defendant never obtained a valid consent to the way it used the users' data which would satisfy the mandatory legal requirements within the meaning of s 2A(a) DPA (and/or Article 7(a) of directive 95/46/EC, corresponding to section 8 para 1 subpara 2 *DSG,* Austrian Data Protection Act). Defendant may plead other legitimate reasons (specifically contractual performance within the meaning of s 2A(b)(i) and/or Article 7(b) of directive 95/46/EC, corresponding to section 8 para 3 subpara 4 *DSG,* Austrian Data Protection Act). These would however, if at all, allow only the processing of data which is absolutely necessary to perform the service and no analysis of data beyond that scope (e.g. for advertising, additional services, outsourcing of data processing and cooperations with third parties which are not absolutely necessary) or the sharing of data with third parties. For "sensitive data" which Defendant further processed, s 2B DPA (and/or Article 8 of directive 95/46/EC, corresponding to section 9 DSG, Austrian Data Protection Act) applies mutatis mutandis to the above argument.

85. Irrespective of the legitimate reasons set out in s 2A and 2B DPA (and/or Articles 7 and 8 of directive 95/46/EC, corresponding to sections 8 and 9 *DSG,* Austrian Data Protection Act) the data was processed unlawfully also according to the general principles of s 2 DPA (and/or Article 6 of directive 95/46/EC, corresponding to section 6 *DSG,* Austrian Data Protection Act), since they were not processed "fairly" within the meaning of s 2(1)(a) DPA (and/or Article 6(a) of directive 95/46/EC, corresponding to section 6 para 1 subpara 1 *DSG,* Austrian Data Protection Act, see in particular s 2D(1) DPA). For lack of a determined, clear and specific purpose, the principle of a specified purpose within the meaning of s 2(1)(c)(i) and (ii) DPA (and/or Article 6(b) of directive 95/46/EC, corresponding to section 6 para 1 subpara 2 *DSG,* Austrian Data Protection Act) was violated, for lack of a legal connection between the data processing and the specific purposes, the data were and still are being processed also excessively within the meaning of s 2(1)(c)(iii) DPA (and/or Article 6(c) of directive 95/46/EC, corresponding to section 6 para 1 subpara 3 *DSG,* Austrian Data Protection Act) and longer than is necessary for the purposes within the meaning of 2(1)(c)(iv) DPA (and/or Article 6(e) of directive RL 95/46/EC, corresponding to section 6 para 1 subpara 5 *DSG,* Austrian Data Protection Act).

Evidence: Examination of the parties

As before

If contested, submission of further documents.

Submission of further evidence reserved.

E. Consent by third parties under data protection regulations

86. As outlined in the foregoing, Defendant mostly processes user-generated data it receives from users. This is not only data which the data subjects themselves upload, but personal data uploaded on a large scale by other users. User A can such also upload data of user B, or even data of non-user C. On this point, see the explanations in the Data Use Policy (Enclosure /.C) under the heading "*Information we receive about you*".

87. Defendant also encourages users to share third-party data (see Enclosure ./I). Defendant's system allows "tagging" other users in data (e.g. pictures, videos or posts), using the "check-in" feature to check them in to places (e.g. indicating their whereabouts) or adding them to "groups". All this happens regularly without the data subject's ex-ante consent.

88. The users of Defendant's services are asked to "synchronise" their contact data of other persons from mobile telephones with Defendant's data bases. In doing so, the user's entire directory and all data it contains about third parties is exported and transferred to Defendant's data bases (see Enclosure ./I).

89. Defendant queries active users about other users: Defendant's system, for instance, asks where one knows "friends" from, whether other users have other "friends" who are not yet assigned on *facebook.com* to these other users, and whether the name indicated by the other user is their true name (see Enclosure ./I).

90. In its Data Use Policy, Enclosure ./C, Defendant states that "*of course*, *for information others share about* [the user] *they control how it is shared*." It is not the data subject who can determine whether data concerning him are processed, whether these data are e.g. public (and therefore can be found on the internet) or "private", but the particular user who uploads the data and generally does not have any rights to these data. Defendant then processes these data for its own purposes.

91. Defendant has repeatedly justified this approach by the "social nature" of its services, which however is not educible from any consent requirement according to s 2A DPA (and/or Article 7 of directive 95/46/EC, corresponding to section 8 *DSG,* Austrian Data Protection Act).

92. In some cases, Defendant has also argued that "consent by third parties" (i.e. by the "uploading" user) was a given. This however is contrary to Article 7(b) of directive 95/46/EC which clearly states that the "data subject" (and not any anonymous third party) must give its consent to processing (ex ante).

93. A "general consent" by users to processing all data obtained in the future which are determined and uploaded by any third party fails to meet the criterion of "specific" and "informed" (about a non-foreseeable situation) as well as the requirement that consent can be given effectively only for a given case and/or specific datum and a specific processing. Any such "ex-ante consent" is therefore invalid on account of absolute indeterminateness, according to s 2A(a) DPA (and/or Article 7(a) in conjunction with Art 2(h) of directive 95/46/EC, corresponding to section 4 para 14 in conjunction with section 8 para 1 subpara 2, *DSG,* Austrian Data Protection Act) alone.

94. Defendant grants the concerned users a limited possibility to delete or "hide" information later, which does not alter the fact that data were originally collected without a legal base. Third parties who are not users of *facebook.com* do not have that possibility, if only because they do not have a Facebook account and are not even in a contractual relation with Defendant. In other cases, the data are not visible and therefore not removable for the data subject.

95. If one were to interpret private use generously, it would be theoretically conceivable to consider this processing by private users as being in conformity with the law, to the extent such processing is done exclusively for the purposes of these private users as controllers. Uploading a photo could, for instance, be seen as a "personal or household activity" (within the meaning of Article 3(2) of directive 95/46/EC), if it is shared only with friends. However, also private users such as e.g. Plaintiff, are forbidden to transmit such data for commercial uses (cf. explicitly section 45 para 2 *DSG,* Austrian Data Protection Act). Defendant's system however cannot prevent the latter, since Defendant processes and commercially uses all uploaded data (regardless of who is "data subject", "consenting person" or "uploading person").

96. Moreover, Defendant's – legally unfounded and hence wrongful - further use must be separated from the issue of private use by the contracting parties of Defendant, since it collects and uses data for its own (commercial) purposes without the data subjects' consent – regularly even without their knowledge – or without any other permission: Summarizing and in exaggerating terms, Defendant uses a system that is tantamount to the criminal offence of "receiving and handling" in which it has users supply it with third-party data (excluding private uses, as appropriate), whose legal origin it does not verify or even question, only to use them further commercially for its own purposes without any legal base.

97. A solution conforming to the law would possibly be achieved if Defendant were not to use personal data uploaded by third parties itself, but were to act merely as a processor ("host") and, as the case may be, seek an ex-ante consent to the use of these data from the data subjects concerned (in other words have these data "released" for its own purposes) and use these data for its own purposes only after such permission has been granted.

98. Hence, Defendant has never obtained a valid consent within the meaning of 2A(a) DPA (and/or Article 7(a) of directive 95/46/EC, corresponding to section 8 para 1 subpara 2 *DSG*, Austrian Data Protection Act) to the processing and use of the data "provided by third parties". There is no other identifiable justification for independent data processing by Defendant.

99. Irrespective of the legitimate reasons set out in s 2A and 2B DPA (and/or Articles 7 and 8 of directive 95/46/EC, corresponding to sections 8 and 9 *DSG*, Austrian Data Protection Act), the data were unlawfully processed also under the general principles set out in s 2 DPA (and/or Article 6 of directive 95/46/EC, corresponding to section 6 *DSG*), since they were not or could not be processed *"fairly"* within the meaning of s 2(1)(a) DPA (and/or Article 6(a) of directive 95/46/EC, corresponding to section 6 para 1 subpara 1 *DSG*).

Evidence: Examination of the parties

As before

Screenshots: Request to disclose third-party data, Enclosure ./I

If contested, submission of further documents.

Submission of further evidence reserved.

F. Unlawful data collection via social plug-ins

100. Defendant stores so-called "cookies" on users' computers. Cookies are small text files which are transmitted to Defendant by the user's internet browser (e.g. Internet Explorer, Safari, Firefox) in the background whenever Defendant's servers are called. Through these sent cookies, Defendant is able to associate the source of such calls with a person. The services of Defendant and many other internet services cannot be used unless the cookie function in the user's internet browser is activated.

101. Defendant moreover offers so-called "social plug-ins" which can be in-built and/or integrated by website operators. The most common of these is Defendant's "Like" button: Technically, a "frame" (*iframe*) is cut into a website (see e.g. below the website of the Austrian daily "*Die Presse*", Fig. 7) and then filled by Defendant with this social plug-in (see Fig. 8). For the user, this creates the impression that these social plug-ins are a part of the operator's website (as in Fig. 7), although technically he is visiting and loading two sites (the site of the website operator and "hidden" also Defendant's site).

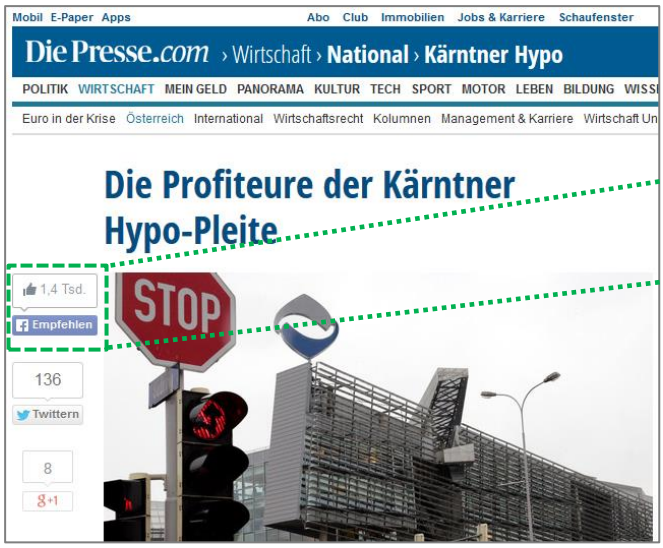

Fig. 7: Integration of the "Like" button on the site of "Die Presse" *Fig. 8: Same "Like" button alone*

102. With every visit of websites which contain Defendant's "Like" button (e.g. that of "*Die Presse*") the stored cookies, the URL of the visited sites and various log data (e.g. IP addresses, dates and times) are transmitted.

103. Defendant thereby records e.g. that "on day X and at time Y user A visited site Z" on the internet. For this the user need not even interact with the "Like" button (e.g. by clicking on it or similar) or notice this button on the website he is visiting. Merely loading a site with such a social plug-in suffices for transmission of such data to Defendant.

104. Aside the fact that users regularly are unaware of these goings-on, they cannot know in advance which sites use such social plug-ins. Social plug-ins are also found on the sites of political parties, on medical websites, sites for homosexuals and even on pornography sites, see by way of example Enclosure ./J. Hence, also "sensitive data" (within the meaning of Article 8(1) of directive 95/46/EC and/or of section 4 para2 *DSG*, Austrian Data Protection Act) are recorded.

105. Defendant describes this data use in its Data Use Policy (Enclosure ./C): *"We receive data whenever you visit (...) or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID".*

106. There is no specific limitation of the purpose of data processing by Defendant, which is why the general clause *"We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use*" applies at any rate. As regards the invalidity of this clause and the invalidity of consent, reference is made to the arguments developed in the foregoing points D. and E.

107. On the storage of these data, Defendant states elsewhere in its Data Use Policy: *"We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days. After that, we remove your name and any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you*". Again, there is no explanation for the purpose of use or the retention period stated. In direct talks with Plaintiff, Defendant explained that this list of all visited websites would be stored for "security reasons" and "important grounds".

108. At another point in the Data Use Policy, Enclosure ./C, Defendant states: "*We use technologies like cookies, pixels, and local storage (…), to provide and understand a range of products and services. Learn more at: https://www.facebook.com/help/cookies* [Annex 1 in Enclosure ./C]. *We use these technologies to do things like make Facebook easier or faster to use; enable features and store information about you (including on your device or in your browser cache) and your use of Facebook; deliver, understand and improve advertising; monitor and understand the use of our products and services; and protect you, others and Facebook. For example, we may use these tools to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners".* This section does not provide for any further limitation of purpose and while the Cookie guideline (Annex 1 to Enclosure ./C) lists seven "categories of use" for the cookies used by Defendant in the context of social plug-ins, these are again broadly framed (e.g. *"provision of products and services")* and again only backed by non-exhaustive examples. As regards the invalidity of this clause, again refer to the arguments developed in the foregoing chapters II.D. and E.

109. Technically, it would be feasible to provide these services without identifying the user through cookies (e.g. by using a URL other than *facebook.com* for the "Like" buttons). Equally, it is possible not to store the technical data (such as IP addresses) needed for transmission, or only in an anonymised format. And it is possible to transmit further data to Defendant only during a (deliberate) interaction with a social plug-in.

110. Hence, Defendant violates the requirement of a specified purpose in s 2(1)(b)(i) and (ii) DPA (and/or Article 6(1) points (c) and (d) of directive 95/46/EC, corresponding to section 6 para 1 subparas 2 und 3 *DSG,* Austrian Data Protection Act), since no specific purpose has been defined for data collection).

111. Defendant further violates the obligation of data minimisation stipulated in s 2(1)(b)(iii) DPA (and/or Article 6 (1) points (c) and (e) of directive 95/46/EC, corresponding to section 6 para 1 subparas 3 and 5 *DSG,* Austrian Data Protection Act), since the data are stored beyond the required extent in terms of scope and period. Ultimately, such a collection of data did not come into being fairly and lawfully and is such contrary to s 2(1)(a) DPA (and/or Article 6 (1) point (a) of directive 95/46/EC, corresponding to section 6 para 1 subpara 1 *DSG*).

112. In all this, Defendant cannot present any legitimate reasons according to s 2A und 2B DPA (and/or Articles 7 and 8 of directive 95/46/EC, corresponding to sections 8 und 9 *DSG,* Austrian Data Protection Act), as processing is neither subject to a valid consent, nor necessary for performing the service nor subject to a legal obligation; neither does it concern the vital interests of a person, nor is it in the public interest nor, let alone, in Defendant's overriding legitimate interest.

Evidence: Examination of the parties

As before

Screenshots, "Like" buttons, Enclosure ./J

If contested, submission of further documents.

Submission of further documents reserved.

G. Unlawful secondary data processing ("big data", data analysis, data association)

113. As outlined above in detail, Defendants collects vast amounts of data about its users and even about third parties which whom it has no contractual relation (so-called "shadow profiles"), thereby using data provided by the users themselves (e.g. status messages or uploaded photos) as well as data of other users (e.g. synchronisation of telephone directories, searches for current cities or friends with other users), additionally buying data from third parties (e.g. data vendors), importing public information (e.g. from Wikipedia) and collecting data itself (e.g. by analysing clicks, meta-data or search requests or tracking data). Defendant interlinks all these data for every user and thereby makes them amenable to processing and analysis. Defendant does not disclose which systems precisely it uses. According to its Data Use Policy however, as good as every use of all data however procured is possible for every conceivable purpose (cf. also the arguments developed under II.D and E. above).

114. Defendant operates analysis systems which fall under the general heading of "big data" using algorithms to explore huge data amounts, to search for correlations and patterns, and to draw conclusions. With "big data" analyses it is possible to "compute" new information (e.g. on sexual orientation, political orientation, state of health or other sensitive user data) from totally uncorrelated information (e.g. a list of friends). Summarizing, new information is generated from totally uncorrelated, partly arbitrarily obtained and often unverified data.

115. Defendant for instance allows advertisers to search for "lookalikes" of existing customers, in other words persons who are similar to existing customers in terms of data (cf. Enclosure ./K), even though these users may have never shown an interest in the advertiser's products. Information on users is also generated from the "Like" statements on *Facebook* pages. The "Like" on Facebook's "evf" ("europe-v-facebook.org") page led to an entry that Plaintiff would be interested in electronic viewfinders (note: e.g. video cameras). The background probably being that the English-language Wikipedia page on "evf" page refers to an article on electronic viewfinders (cf. Enclosure ./L).

116. Defendant uses this information for its own purposes and suggests to users to e.g. add their hometown, current city, school, university or employer. The place where the user probably works is then determined from the existing data (e.g. places of work of friends). In this manner, Vienna was proposed to Plaintiff as current city, his hometown Salzburg as place of birth, his

high school in Salzburg as school and Vienna University as university, without Plaintiff actually having provided this information himself. Obviously, similarities with "friends" on Facebook were used (Enclosure ./M).

117. In one project, Defendant even calculated whether the partnerships of users would last (Enclosure ./N). In external analyses, the sexual orientation, drug consumption or political views of users were calculated from (scarce) information which had been made public (Enclosure ./O).

118. Defendant does not limit data analysis by time-related, thematic or other criteria (e.g. "only publicly retrievable text messages from the past 30 days"), but takes the liberty to process all data from all sources, regardless of the original purpose, for any other purpose. This tantamount to "unrestricted dragnet investigation".

119. Summarizing, Defendant processes data beyond the scope of any related purpose and downright systematically and deliberately violates the requirement of a specified purpose according to s 2(1)(b) DPA (corresponding to Article 6(b) of directive 95/46/EC and/or section 6 para 1 subpara 2 *DSG,* Austrian Data Protection Act).

120. Moreover, using data from any source for any purpose is clearly disproportionate and therefore in violation of s 2(1)(b)(iii) [TN8] because "*excessive*" (corresponding also to Art 6(c) of directive 95/46/EC, see also section 6 para 1 subpara 3 in conjunction with section 7 para 3 *DSG,* Austrian Data Protection Act). On this point, reference is made in particular to the case law of the CJEU in C-293/12 and C-594/12 and, amongst others, of the Austrian Constitutional Court in G62/2012 which has ruled that even retaining traffic data for the purpose of fighting terrorism is a violation of Article 8 of the EU Charter of Fundamental Rights (Charter) and of Austrian constitutional law. The unrestricted processing of content data for the purpose of boosting advertising revenues, which is far less worthy of protection, appears to be all the more disproportionate, if only on the basis of Article 8 of the Charter.

121. Besides, Defendant is violating the obligation of data minimisation stipulated in s 2(1)(b)(iii) DPA (and/or Article 6(1) points (c) and (e) of directive 95/46/EC, corresponding to section 6 para 1 subparas 3 and 5 *DSG,* Austrian Data Protection Act), since the data are stored beyond the required extent in terms of scope and period. Finally, any such collection of data did not come about fairly and lawfully; it is therefore contrary to s 2(1)(a) DPA (and/or Article 6(1) point (a) of directive 95/46/EC, corresponding to section 6 para 1 subpara 1 *DSG,* Austrian Data Protection Act*)*.

122. In this context as well, a legitimate reason within the meaning of s 2A and 2B DPA (corresponding to Articles 7 and 8 of directive 95/46/EC and sections 8 und 9 *DSG,* Austrian Data Protection Act), cannot be made out. Specifically, consent to the processing of next to "all data from all sources for every type of analysis" will not be legally effective.

Evidence: Examination of the parties

As before

Defendant's statement on "Lookalike" analysis, Enclosure ./K

Printouts: data download and Wikipedia, Enclosure ./L

Screenshots, Defendant's proposals, Enclosure ./M

Report, A Network Analysis of Relationship Status on Facebook, Enclosure ./N

Report, Private traits and attributes are predictable from digital records of human behavior, Enclosure ./O

If contested, submission of further documents.

Submission of further documents reserved.

H. The "Graph Search" function

123. In March 2013, Defendant introduced a search function called "Graph Search" which allows performing a "dynamic search" of the hitherto static data users could access. With this function, all data of other persons or pages which the user was able to see but could only find with difficulty in the past have become searchable.

124. This massively heightens the intensity of interference as well as the likelihood that erroneous settings (e.g. making data "public") have a practical consequence. In addition, data which were provided by the user for self-presentation or other purposes only (e.g. signing up for an event) are now used and "converted" for a new purpose, namely the Graph Search function.

125. The search results in first trials were most problematic: one could, for instance, retrieve a list of homosexuals in Iran or Falun Gong supporters in China. Other questionable searches can be performed as well. One finds e.g. persons who are married and like prostitutes, or employers of persons who are in favour of "racism" and/or also those employees themselves (c.f. examples in Enclosure ./P). Even with less problematic queries (e.g. all persons working with company X, all persons who like company X) are possible with Graph Search. As regards the separation of data retention and search, and the higher degree of interference, reference is made also to the CJEU's "Google" judgment C-131/12.

Lacking consent / Opt-out ignored

126. At no time whatsoever did Defendant seek the consent of users to this new form of data processing, but it initiated this form of data use arbitrarily and unilaterally.

127. Until Graph Search was introduced, Defendant had at least given users the option not to appear in any search engines "*on and outside of Facebook*" (see Fig. 8). Plaintiff had selected this option.

Fig. 8: Old objection form ("opt-out") from any search engines

128. After having introduced Graph Search, Defendant however changed the text in the check box which suddenly spoke of "other search engines" only.

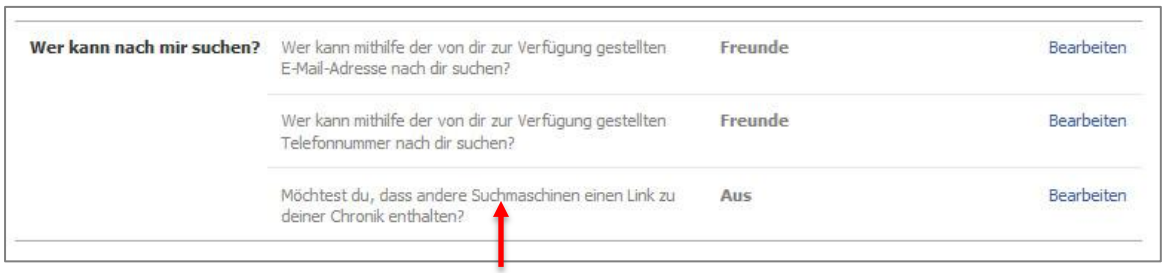

Fig. 9: New objection form ("opt-out") from "other" search engines

129. Against Plaintiff's explicit wish not to appear *in any* (i.e. not even in an internal Facebook) search engine *whatsoever*, a different content was deceitfully planted into the statement subsequently and Plaintiff's instruction was restricted to "*external search engines*" (such as Google, Bing, Yahoo). Contrary to his explicit objection, Plaintiff's data are now contained in Graph Search and searchable and accessible for other users.

130. Summarizing, Defendant processes data beyond the original purpose and such violates the requirement of specified purpose of s 2(1)(b) DPA (corresponding to Article 6(b) of directive RL 95/46/EC and/or section 6 para 1 subpara 2 DSG, Austrian Data Protection Act).

131. Moreover, a legitimate reason within the meaning of s 2A and 2B DPA (corresponding to Articles 7 and 8 of directive 95/46/EC and sections 8 and 9 *DSG,* Austrian Data Protection Act) cannot be made out. In particular, consent to processing is legally ineffective.

132. Finally, any such collection of data (if only because of the subsequent alteration of the content of the statement of intent expressing Plaintiff's opt-out) was not generated fairly and lawfully and is therefore contrary to s 2(1)(a) DPA (and/or Article 6(1) point (a) of directive 95/46/EC, corresponding to section 6 para 1 subpara 1 *DSG*, Austrian Data Protection Act).

Evidence: Examination of the parties

Examples on "Graph Search", Enclosure ./P

If contested, submission of further documents.

Submission of further documents reserved

I. Unlawful transmission to external "applications"

133. Defendant allows users to link their Facebook accounts with software programs by third-party providers ("apps"). Via a programming interface, users can transmit large volumes of data to these third-party providers ("app operators").

134. Defendant allows users to also share the data of other users with these app operators such as friends lists, or all "friends" data which the users can view, private messages between the user and third persons and many other data categories.

135. Defendant does not inform these users thereof in any manner whatsoever and does not seek their consent. Only a general consent is given via Defendant's Data Use Policy (Enclosure ./C). Users however cannot anticipate which "friend" will share which data with which third person for what purpose.

136. It is only in the fifth (!) sub-menu of the *Facebook* page (Account Settings > Settings > Apps > Apps you use / Edit > Disable, see Enclosure ./Q) that users can de-activate this function (opt-out). Consent (opt-in) is not sought by Defendant. However, if the user deactivates this function, he himself can no longer use apps and the features of the *Facebook* platform. It is not possible to deactivate the use of one's own data by third parties ("all-or-nothing" principle).

137. Users can limit, but not fully prevent, access by apps of other users by deleting (opting-out) 17 (!) individual "ticks" (see page 6 of Enclosure ./Q). This option is likewise located in the fifth sub-menu of the settings. Here, Defendant has partly introduced and activated new "ticks" (see screenshot Enclosure ./R) even though Plaintiff had deleted and/or deactivated all ticks earlier.

Responsibility for data processing

138. Again, the distribution of roles under data protection rules is unclear here. One must assume that it is primarily the user who is the controller of the transmission, and that Defendant as processor provides the required data of other users (the "friends" of the user in question), without being sufficiently entitled to do so. As processor for those users, Defendant stores all data of these users only to use them abusively for its own purposes, or at best upon the instruction of another user. Defendant then benefits from higher interaction, additional advertising or payments for the use of apps.

Other measures by Defendant

139. Defendant has special provisions governing external app operators (Enclosure ./S). Looking merely at their degree of determinateness, these provisions are to all practical intents unsuitable for ensuring a use of data by third-party operators which conforms to data protection regulations. One must not forget that these third-party operators are spread around the whole world: Anybody can set such apps without prior verification. There are hundreds of thousands of apps on *facebook.com*. A review conducted in 2011 found that the then largest app provider *Zynga* did not even meet the most primitive requirements of Defendant (e.g. link to data protection guidelines). The enforcement of other provisions (e.g. deletion of data) with anonymous and globally spread providers which all have their own (often virtual) infrastructure is hence an utter illusion.

140. Summarizing one can state that, in contravention of its duties as processor, Defendant makes available data it administers for Plaintiff as controller to other controllers, without the consent and even against the explicit instruction of Plaintiff and therefore violates its duties according to s 2C(3)(a) and s 21(1) DPA (and/or Article 16 and 17 of directive 95/46/EC, corresponding to section 11 para 1 subpara 1 and section 14 *DSG*, Austrian Data Protection Act).

141. Moreover, such transmission to (often factually unknown third parties) which are largely found in countries which do not afford an "adequate level of protection" within the meaning of Article 25 of directive 95/46/EC is unlawful under s 2, 2A and 2B DPA (corresponding to Articles 6, 7 and 8 of directive 95/46/EC), since there is neither a legitimate reason, nor are the requirements of lawful processing satisfied.

142. Inasmuch as Defendant were to invoke its own controllership, it is violating in particular the requirement of specified purpose in s 2(1)(b)(i) and (ii) DPA (corresponding to Art 6(a) of directive 95/46/EC and section 6 para 1 subpara 2 *DSG,* Austrian Data Protection Act) and the duty of "*fair*" processing in s 2(1)(a) in conjunction with s 2D(1) DPA (corresponding to Article 6(a) of directive 95/46/EC and section 6 para 1 subpara 1 DSG, Austrian Data Protection Act*).*

Evidence: Examination of the parties

As before

Screenshot, deactivation of app access, Enclosure ./Q

Screenshot, Defendant added new permissions, Enclosure ./R

Provisions for developers, Enclosure ./S

If contested, submission of further documents.

Submission of further evidence reserved.

J. Unlawful data transmission to the U.S.A. ("PRISM")

143. According to its own information, Defendant relies on its parent company "*Facebook Inc.*" (1601 Willow Road, Menlo Park, CA 94025, USA) as processor when using and processing user data. Facebook Inc. operates server centres itself and uses further sub-contractors.

144. Pursuant to Article 25 of directive 95/46/EC the transmission of data into countries outside of the European Economic Area is admissible only if the target state achieves an "adequate level of protection". In simplified terms this means that the third country must have data protection laws in place which are comparable to directive 95/46/EC, which can be determined by the EU Commission in a general administrative law decision.

145. Data protection does not exist in the U.S.A. within the European meaning and the U.S.A. therefore does not offer an "adequate level of protection". By way of decision 2000/520/EC of 26 July 2000 ("Safe Harbour" decision) the European Commission has nevertheless recognized a "self-certification system" run by the U.S.A. as an "adequate level of protection" within the meaning of the directive. This recognition by the Commission dates before 11 September 2001 and the legislative and factual changes which followed in the U.S.A thereafter.

146. Under this "Safe Harbour" system US companies may commit on a voluntary basis to comply with "principles" which are modelled on EU data protection. It is monitored by private control bodies ("TRUSTe" in the case of *Facebook*). Under the heading of unfair business practices, the US authorities (in particular the Federal Trade Commission) may also sanction violations of this self-commitment, but they are under no obligation to do so.

147. Under the "onward transmission" principle (Annex 1 to the Safe Harbour decision) transmitting data of third parties is forbidden. However, under the heading of "Principles" (Annex 1 to the Safe Harbour decision) adherence to the Safe Harbour principles is limited in the areas of "national security", "statutory law" or "common law". The prevailing view in the EU is however that those restrictions apply only within the limits of what is absolutely necessary. For this reason, in particular involvement in "mass surveillance" concurrently with self-certification

under Safe Harbour is unlawful (cf. e.g. Communiqué of the European Commission of 27 November 2013, letter of the Article 29 Working Party of 13 August 2013, comment by the EDPS of 7 October 2013, letter of the German data protection authorities of 24 July 2013, report by EU-US working party of 27 November 2013 and WP 215 of the Article 29 Working Group, Enclosure ./T)

148. The unlawfulness results also from the interpretation of the Safe Harbour decision in conformity with the directive and primary law. In C-465/00 (*Österreichischer Rundfunk* et al.) the CJEU already ruled that directive RL 95/46/EC must be interpreted in the light of Article 8 ECHR. Under the Lisbon Treaty, Articles 7 and 8 of the European Charter of Fundamental Rights (Charter) are additionally relevant in the interpretation of secondary law acts.

149. On 6 June 2013, the general public learned about the PRISM surveillance programme of the US National Security Agency (NSA) through the disclosures by whistleblower and former secret service staff member Edward Snowden in various newspapers (such as *The Guardian, Washington Post, Der Spiegel*). It was proven in published files that a number of US companies had given the NSA access to their server systems (Enclosure ./U). "*Facebook*" is explicitly mentioned in these files. According to the files, involvement began on 3 June 2009 (page 4 in Enclosure ./U). The code for the data from the *Facebook* systems is "P4" (page 7 in Enclosure ./U). The files of the NSA's "*XKeystroke*" programme, which was disclosed later, also show that Facebook data were analysed (pages 11 and 12 in Enclosure ./R).

150. The U.S.A have repeatedly admitted to and defended the existence of the PRISM programme in public. The companies concerned, including *Facebook Inc,* first denied any involvement and stated unanimously that they had no knowledge of the programme. There is no logical explanation how the PRISM programme can undisputedly exist, but allegedly none of the concerned companies participated or participate. However, the affected US companies are subject to a statutory duty of non-disclosure ("gag order") and must therefore deny any involvement by virtue of the law. In a public hearing of the Privacy and Civil Liberties Oversight Board, US government representatives stated under oath that all companies concerned had received a court order and were fully informed (cf. also Enclosure /.V). This is also in conformity with the legal requirements in the U.S.A.

151. The form of surveillance under PRISM is "mass surveillance", which in particular is not subject to any concrete initial suspicion, judicial control or other similar limitations under the rule of law. In the U.S.A., "mass surveillance" is allowed under section 702 of the FISA Amendment Act (now 50 U.S.C. section 1881 et seq.). Judicial review in individual cases it not provided for.

152. Equally, there are no legal remedies for affected persons. At the level of constitutional law either, there is no protection in the U.S.A. for foreigners, as the US Constitution does lay down (limited) fundamental rights to privacy, but only for US citizens or persons having their permanent residence in the U.S.A. (concept of "civil rights").

153. In the U.S.A, the surveillance laws of course take precedence over the self-commitment under Safe Harbour. The control body commissioned by *Facebook Inc* under Safe Harbour (True

Ultimate Standards Everywhere Inc, 835 Market Street, Suite 800, San Francisco, USA *"TRUSTe")* answered accordingly that they had no possibility or competence to take action against PRISM (see email of 2 Dec 2014 as Enclosure ./W)

154. All in all, one can clearly establish that in the present case an "adequate level of protection" within the meaning of Article 25 of directive 95/46/EC is not afforded when Defendant transmits personal data to the U.S.A. The requirements of the Safe Harbour decision are not complied with by the recipient in the U.S.A. (*Facebook Inc*) and cannot be verified and enforced by the competent control body. This conclusion is also backed by an interpretation of Article 25 of directive 95/46/EC in conformity with the fundamental rights, as well as by the European Commission's earlier Safe-Harbour decision.

155. However, Defendant was under an obligation according to s 2C(3)(c) DPA (and/or Article 17 para 2 of Directive 95/46/EC, corresponding to section 10 para *1 DSG,* Austrian Data Protection Act*)* to assure itself of whether the processor (*Facebook Inc*) was actually complying with the self-commitment. Given the scope of the data transmission it was and is irresponsible to "blindly" trust in self-certification (e.g. registration on a list). After all, Defendant was outsourcing the data processing for over 1 billion data subjects to this processor. At the time the PRISM scandal was revealed in June 2013 at the latest, instant measures should have been taken to end any further transmission of user data to the U.S.A. However, Defendant did nothing and continues to unlawfully transmit personal data to its processor in the U.S.A. where they are used by the US secret service, in particular the NSA.

156. Data transmission is and was unlawful according to s 11 DPA (and/or Article 25 of directive 95/46/EC, corresponding to sections 12 and 13 *DSG,* Austrian Data Protection Act) for lack of an adequate level of protection (in the given case in the U.S.A.). Furthermore, Defendant did not ensure that the processor used (*Facebook Inc*) satisfies the legal requirements of s 2C(3) and s 21 DPA (and/or Article 17 of directive 95/46/EC, corresponding to sections 10 and 14 *DSG,* Austrian Data Protection Act).

157. On top of that, the data were also used beyond the original purpose ("social network" turned into "mass surveillance"); Defendant such violates the requirement of a specified purpose of s 2(1)(b) DPA (corresponding to Article 6(b) of directive 95/46/EC and/or section 6 para 1 subpara 2 *DSG,* Austrian Data Protection Act). Moreover, no legitimate reason within the meaning of s 2A and 2B DPA (corresponding to sections 7 and 8 of directive 95/46/EC and sections 8 and 9 *DSG,* Austrian Data Protection Act*)* can be made out.

Evidence: Examination of

- Mr Edward Snowden, born 21 June 1983, as witness, pA c/o Wolfgang Kaleck, attorney at law, Immanuelkirchstrasse 3–4, D-10405 Berlin, by way of mutual legal assistance, if necessary
- Mr Glenn Greenwald, born 6 March 1967, as witness, pA Freedom of the Press Foundation, 603 Van Ness Ave. Suite E731, San Francisco, CA 94102

- Mr Barton Gellman, born 1960, as witness, pA The Washington Post, 1150 15th Street NW, Washington DC 20071, USA
- Mr Marcel Rosenbach, born 1972, as witness, pA Der Spiegel, Ericusspitze 1, D-20457 Hamburg
- Mr Holger Stark, born 1970, as witness, pA Der Spiegel, Ericusspitze 1, D-20457 Hamburg

Statements on the admissibility of mass surveillance under the "Safe Harbour" decision, Enclosure ./T

Documents by Edward Snowden on PRISM and XKeyStroke, Enclosure ./U

Transcript of PCLOB of 19 March 2014, Enclosure ./V

Reply by TRUSTe, Enclosure ./W

If contested, submission of further documents.

Submission of further evidence reserved.

K. Defendant's duty to provide information

158. In early June 2011, on 9 November 2011, and on 27 October 2012, Plaintiff sent a request for information within the meaning of s 4 DPA (and/or Article 12 of directive 95/46/EG, corresponding to section 26 *DSG,* Austrian Data Protection Act*)* to Defendant concerning the processing of his personal data. In the course of extensive e-mail correspondence (Enclosure ./X) he received a first pdf-file of 18 pages on 9 June 2011 (Enclosure ./Y), which according to Defendant contained *all* data. Retrospectively, compared with the then following further answer, it covered only approx. 1.5 % of all data (by page volume).

159. Following further interventions by Plaintiff, Defendant's parent company (*Facebook Inc*.) sent a CD ROM with another pdf-file of 1,222 A4 pages, although Defendant had repeatedly maintained earlier that all data had already been disclosed.

160. After further intervention and a complaint addressed to the Irish Data Protection Authority (a decision thereon is still pending) Plaintiff received another e-mail on 28 September 2011 (Enclosure ./Z) clarifying that no further data would be stored. This notwithstanding, Defendant later conceded the existence of further data (e.g. facial recognition data).

161. Defendant did not respond to any subsequent requests for information and referred Plaintiff (by way of automatically generated email) to a "download tool" (1), an "advanced download tool" (2), his own profile (3), his "activity log" (4) and some other points of reference (5) on *facebook.com*. Instead of actively providing a reply, Defendant sent Plaintiff on a "paper chase" in obtain his data. Ever since, Defendant has refused to make any further disclosures to Plaintiff.

162. On verification, Plaintiff found the cited data references to be flawed (e.g. data were for the most part lacking in the "activity log"), apparently deliberately trimmed (e.g. cookie data were largely replaced by "…"), at any rate they were found to be wanting.

163. Numerous tests and a comparison of the different data sources have clearly shown that to date Defendant has made available only fractions of the data about Plaintiff it processed, even though it had at every instance assured to provide "full information".

164. If one compares the data which (theoretically at great effort) can be accessed via the access points indicated by Defendant with the sent pdf-files, with the data which are apparently required for the platform to function and with Defendant's various activities, it is also clear that Defendant has made accessible only a part of the data and that there is an obvious inconsistency in the replies given to the requests for information. On this, see also a table which compares the answers provided so far in Enclosure ./AA.

165. Without disclosure by Defendant, Plaintiff is unable to submit a final list of all data which were recorded, collected, stored, transmitted or processed in any other form by Defendant. It is rather on Defendant to produce a list of all data on Plaintiff it processed and, as appropriate, to bring forward and prove exceptions from the duty to provide information.

Information on purposes, source, recipients and logical structure

166. Failing to comply with its obligation, Defendant did not provide Plaintiff with information on the purpose, the sources and the recipients of transmissions. Likewise, Defendant did not disclose the existence or logics of any analyses. Moreover, various "codes" in the data were not explained. Defendant did, however, refer to the vague information in its Data Use Policy (Enclosure ./C), as above. To date, Defendant has not provided any information on the purpose, sources and recipients of the data and their use by Defendant.

167. Summarizing, 3 years after the first request for information, Defendant has not provided sufficient information on the purposes of data processing, the sources, recipients or logical structure of the processed data , in spite of a deadline of a maximum of 40 days provided for in the Irish implementing law (cf. s 4(1)(s) DPA). Neither has Defendant to this day transmitted a full copy of the processed data.

Evidence: Examination of the parties

As before

Correspondence concerning request for information, Enclosure ./X

First reply of 18 July 2011, Enclosure ./Y

Further reply of 28 September 2011, Enclosure ./Z

List of Defendant's data, Enclosure ./AA

If contested, submission of further documents.

III. Applicable law

168. Plaintiff does not fail to recognize the principles of "*iura novit curia*" and "*da mihi factum, dabo tibi ius*". Given the complexity of the facts (across national borders and legal systems), it still seems expedient to examine the applicable law from Plaintiff's perspective.

A. Applicable data protection law

169. According to Article 20 Rome Convention on the law applicable to contractual obligations (Article 23 Rome I Regulation) special legal provisions in EU law (*lex specialis*) prevail over the general rules of the Rome Convention and the Rome I Regulation. Article 4 of the relevant directive 95/46/EC ("data protection directive") stipulates that the governing law at the registered office of the controller is applicable. Data protection law therefore is not amenable to a choice of law.

170. Accordingly, similar provisions are laid down in section 3 para 1 of the Austrian Data Protection Act (DSG) and in s 1(3B) of the Irish Data Protection Act (DPA) by which directive 95/46/EC was implemented.

171. Consequently, Defendant is governed by Irish data protection law, Plaintiff (to the extent he acts as controller) by Austrian data protection law, and further users by their respective national data protection laws. Indirectly at least, both parties are therefore subject – inasmuch as the directive is not directly applicable – to directive 95/46/EC ("data protection directive"). For a simplified overview, see the correlation table (directive 95/46/EC, Austrian Data Protection Act, Irish Data Protection Act) in Enclosure ./AB.

B. Applicable civil law

172. The governing law is derived (depending on the time the contract was concluded) either from the Rome Convention on the law applicable to contractual obligations or from the Rome I Regulation. In the case at hand, both result in the same applicable law, which is why both legislative texts are referred to in the following.

173. Under Article 3 Rome Convention (Article 3 Rome I Regulation), the governing civil law is subject to a free choice of law by the parties. In section 16.1 of its Statement of Rights and Responsibilities (see Enclosure ./A), Defendant chose the law of the US state of California to govern the legal relation between users and itself.

174. Under Article 10 Rome Convention (Article 12 Rome I Regulation), the choice of law (contractually agreed law) does not only govern rights arising from the contract itself, but also all factually related claims (in particular for damages), irrespective of the qualification of the claim under national law.

175. Under Article 5(2) Rome Convention (Article 6(2) Rome I Regulation), this choice of law does not apply if the *ius cogens* in the respective consumer state is more favourable. Moreover, Article 7 Rome Convention (Article 9 Rome I Regulation) limits the applicable law by the overriding mandatory rules of the *lex fori* (i.e. Austrian law). Ultimately, Article 16 Rome Convention (Article 21 Rome I Regulation) allows refusing the application of law which is contrary to public policy of the *lex fori*.

176. Given Defendant's choice of law, Californian law generally applies to civil-law claims between Plaintiff (and/or the originally entitled assignor, cf. IV.C. of this Statement of Claim) and Defendant which are factually related to the contract. This is limited only by the *ius cogens* of the respective consumer state and overriding mandatory rules as well as public policy under Austrian law.

177. As regards users residing in Germany, Defendant chose (by way of exception) German law in an annex to section 17.3 of its Statement of Rights and Responsibilities. These are therefore generally governed by German civil law.

178. Under Article 3 of the Rome I Regulation, the assignments outlined in chapter IV. C. between other consumers and Plaintiff are governed by Austrian law by virtue of choice of law (cf. Enclosure ./AC).

179. Under Article 12 Rome Convention (Article 14 Rome I Regulation), the assignability of claims between other consumers and Defendant must be assessed in accordance with the law applicable to this contract. This is why, given Defendant's choice of law, Californian law applies, limited only by the *ius cogens* of the respective consumer state and overriding mandatory rules as well as public policy under Austrian law.

Evidence — Examination of the parties

As before

Correlation table, Enclosure ./AB

Declarations of assignment, Enclosure ./AC

If contested, submission of further documents.

Submission of further evidence reserved.

IV. Claims from infringements of the law

A. Plaintiff's original claims for damages and on account of unjust enrichment

180. By the infringements set forth in II. C to J above, Defendant has systematically, wilfully and wrongfully interfered with Plaintiff's (constitutionally protected) rights to data protection and privacy, thereby causing damage to him.

181. As stated above, civil-law claims between Plaintiff and Defendant are primarily governed by Californian law, given the chosen law (see III.A).

182. In the U.S.A., the law of damages is generally a matter of the federal states. Compensation for damage ("torts") is largely not statutory law, but part of US judge-made law ("common law").

183. Under the Californian law of torts, four elements must be met to give rise to a claim to compensation: a legally recognized duty ("duty"), a breach of this duty ("breach"), "causation" and "damage". The first two elements ("duty" and "breach") together are equivalent to the notion of wrongfulness ("*Rechtswidrigkeit*") under Austrian law, the elements of "causation" and "damage" correspond to elements by the same name in Austrian law.

184. Under Californian law there is no specific compensation for damage for "violation of data protection" since the notion of data protection in the European meaning is alien to U.S. law. If, however, there is a liability claim ("cause of action") outside the scope of Californian law (e.g. regularly in a U.S. federal law and/or in the present case in directive 95/46/EC), the general rules of *common law* apply to compensation for damage under prevailing doctrine and established case law. Loopholes in compensation for damage must at any rate be closed. Along these lines, section 3523 of the California Civil Code stipulates: "*For every wrong there is a remedy*".

185. If such remedies are lacking in *common law*, the closest related claim to compensation *("tort")* which exists in common law must be applied (cf. e.g. Witkin, Summary of California Law, 10th, 5 Torts, sections 12 and 13, and with further references).

186. Whether any such liability claim exists under a law must be assessed according to the intentions of the respective lawmaker (*"legislative intent")* (cf. e.g. Witkin, Summary of California Law, 10th, 5 Torts, section 13).

187. As Articles 22 and 23 of Directive 95/46/EC explicitly provide for such a claim to compensation (as well as for the possibility of private enforcement ("express cause of action")), these requirements as well as that of wrongfulness ("duty" and "breach") are satisfied at any rate.

188. Californian law does *not* differentiate between material and immaterial damages. Any harm suffered through an unlawful act of a third person gives rise to a claim to compensation (cf. sections 3281 to 3282 and 3333 California Civil Code).

189. In the case of an individual's *invasion of privacy*, not only the positive damage, but also the *emotional distress* and generally the *interest in privacy* are amenable to compensation. This implies that any wrongful immaterial impairment is fully amenable to compensation (cf. e.g. Witkin, Summary of California Law, 10th, 6 Torts, section 1548 et seq. and section 1704, with further references; Restatement of Torts, Second, section 652H).

190. As set out under II., Defendant has at several instances and systematically violated the laws to which it is subject ("duty" and "breach") and has therefore caused ("causation") an impairment to Plaintiff's right to privacy ("damage"). Plaintiff therefore has a claim to immaterial damages.

191. Alternatively, Plaintiff is basing his claims also on section 33 para 1 *DSG 2000* (Austrian Data Protection Act 2000) and on section 1328a *ABGB* (Austrian General Civil Code) and on the direct applicability of Article 23 of directive 95/46/EC, which – in contrast to Austrian law (and the law of a number of other Member States) – does not provide for any limitations to compensation for immaterial loss sustained.

192. According to prevailing doctrine on section 1328a *ABGB* a contractual obligation not to disclose facts relating to a person's private sphere is generally owed as performance, so that the burden of proof according to section 1298 *ABGB* rests on the obligor. Since Defendant had committed itself in its Statement of Rights and Responsibilities, Enclosure ./A to respecting the privacy of Plaintiff (and of all other users), Defendant will have to prove in the case at hand that it complied with the required duty of care.

193. As set out under II. C to J, Defendant processed (and is still processing) data of Plaintiff wrongfully. Defendant uses data of Plaintiff without title for its own purposes and generates considerable advantages therefrom. It bases its business model, as set out under II. A., essentially on the wrongful use of data such as those of Plaintiff. As regards unjust enrichment, Plaintiff is basing his claims against Defendant on Californian law, and alternatively on section 1041 *ABGB*. The said provisions grant the entitled ("harmed") person a claim on account of unjust enrichment (claim for profitable utilization) for his property being wrongfully used for the benefit of another (the enriched person). Defendant has enriched itself by the wrongful use of Plaintiff's data and is under an obligation to surrender the advantage gained.

194. The wrongful commercial use of data and the wrongful transfer to the U.S.A. has in fact generated considerable direct and indirect financial advantages for Defendant and, specifically, has substantially raised the value of its company.

Evidence: Examination of the parties

As so far

Data to be submitted by Defendant

Submission of further evidence reserved.

Amount of compensation claim

195. In comparable cases, the courts assessed the following sums: In *Chitraker v. Bell TV* the Canadian Federal Court awarded under a Canadian act corresponding to directive 95/46/EC an amount of CAD 10,000 (approx. EUR 6,500) as compensation for immaterial loss and another CAD 10,000 as punitive damages for the one-time unlawful search with a commercial credit agency. In *Halliday v. Creation Consumer Finance Limited* the British Court of Appeals awarded BGP 751 (approx. EUR 900) under directive 95/46/EC in terms of immaterial damages for a single incorrect entry with a commercial credit agency. In Austria, compensation for sustained grievance in the amount of EUR 750 was considered justified in 6 Ob 247/08d for the one-time disclosure of credit information.

196. The law chosen by Defendant provides for statutory lump-sum compensations for damage which is difficult to quantify. U.S. or Californian law, for instance, stipulate US 100 to USD 10,000 (approx. EUR 72 to EUR 7,275) for intercepting and using confidential communication per day of surveillance, at least USD 750 (approx. EUR 545) for the right to the protection of one's own image, name and similar, and a minimum of USD 1,000 (approx. EUR 725) for wrongfully transmitting data stored with internet services.

197. The law chosen by Defendant allows awarding punitive damages in addition. In contrast to U.S. common law, section 3294 California Civil Code limits punitive damages to cases of wilful violation of the law ("malice"), which is clearly given in all of the above cited infringements. Moreover, the U.S. Supreme Court has developed flexible moderation in the framework of the U.S. Constitution, which has been determined at approx. the tenfold of the primary loss, as the case may be.

198. Punitive damages under Californian law fulfil several functions: similar to liquidated damages under Austrian law, they are to ensure compliance with the law (punitive element). Liquidated damages may also be agreed in Austria and are subject to the judge's right of moderation, as the case may be. However, one should not forget that Defendant intentionally chose a law which is

known to allow extensive compensation claims and hence appears to be worthy of protection to a very limited extent only. In addition, U.S. punitive damages also skim off the profits from the breach of the law, which corresponds to the more inoffensive function of the Austrian law on unjust enrichment. Moreover, punitive damages also develop criminal-law functions, which do not exist in this form in Austrian civil law.

199. Considering the legal situation in combination with existing case law, the immaterial loss for interference with Plaintiff's rights would have to be assessed at a range from approx. EUR 500 to EUR 7,000. Out of procedural caution, Plaintiff has assessed his claims under the title of compensatory damages and punitive damages under Californian law, and/or under section 33 para 1 *DSG* 2000 (Austrian Data Protection Act) and 1328a *ABGB* (General Civil Code) and Article 23 of directive 95/46/EG at EUR 500 – subject to further extension – plus the claim to profitable utilization to be determined.

Evidence: As before

Expert opinion possibly to be commissioned in the area of business management and auditing on the issue of an adequate usage fee / ascertainment of the advantage which Defendant gained from the wrongful use of the data.

Ineffectiveness of the exclusion of liability

200. In section 16.3 of its Statement of Rights and Responsibilities, Enclosure ./A, Defendant has stipulated *an exclusion of liability* for any claim in excess of USD 100. Any such general exclusion of liability is invalid even under the law chosen by Defendant (section 1542 California Civil Code). In its Statement of Rights and Responsibilities, Defendant states that users hereby waive this prohibition of an exclusion of liability, but does so only for users residing in California (English version) or citizens of California (German version), so that Plaintiff and other users who in fact do not have their place of residence in California and/or are not "citizens" of California are not covered by this waiver of the prohibition of the exclusion of liability and can therefore invoke section 1542 California Civil Code without any problems.

201. In this context, it is needless to take a look at any mandatory provisions and overriding mandatory rules under Austrian law (in particular as regards *contra bonos mores* pursuant to section 879 *ABGB* (General Civil Code) and section 6 *KSchG* (Consumer Protection Act)) and according to Austrian public policy regarding any such exclusion of liability.

B. Assigned claims for compensation and on account of unjust enrichment (excluding German users)

202. Other consumers (who are likewise users of the services and therefore contracting parties of Defendant) have transferred their claims to compensatory damages, punitive damages and on

account of unjust enrichment, to Plaintiff by way of assignment, based on essentially identical facts. In the present Statement of Claim, Plaintiff's original claims are therefore asserted together with the claims assigned by third parties to Plaintiff and/or pooled in a class action under Austrian law.

203. A total of six users of Defendant's services having their place of residence in Austria and in India have assigned their claims arising from the infringements committed against them to Plaintiff.

204. Regarding claims under the title of compensation for damage and on account of unjust enrichment, the situation of these users is the same as that of Plaintiff. As to wrongfulness, reference is made to chapter II. As to the entitlement to compensation for damage, reference is made to chapter IV.A.

205. For reasons of procedural caution, the assigned claims under the title of compensatory damages and punitive damages – and subject to further extension – plus the claim to profitable utilization to be determined have been quantified at EUR 500 each. In aggregate, the claims assigned therefore amount to six times EUR 500, and adding those on account of unjust enrichment, to EUR 3,500. Plaintiff has reserved the right to extend the claim stated (also considerably as the case may be) should further claims be assigned to him.

206. In all this it is recognized that claims to compensation ("torts") are generally not assignable under Californian law. This is justified by public policy which must ensure that claims to compensation would not become a tradable good, the major fear being that consumers could assign their claims to attorneys or debt collection agencies and be subsequently compensated for only a minimal portion of the actual loss suffered.

207. In the case at hand, the assignment is not aimed at realising the loss sustained by the harmed persons (e.g. factoring), but only at joint enforcement. Joint enforcement is recognized in the U.S.A. ("*class action*"), for which the individual entitled person's consent may not even be required. Under U.S. law, actions are pooled at procedural level in contrast Austrian law where they are pooled at substantive law level ("class action under Austrian law").

208. The interaction of the legal systems results in a conflict of values: Both legal systems allow for a "class action", yet the prohibition of assignment under substantive Californian law and the impossibility of a procedural "class action" under Austrian law create a gap which is contrary to the common *ratio legis* of both legal systems.

209. Under concurring case law and doctrine (e.g. *Neumayr* in *Koziol/Bydlinski/Bollenberger*, ABGB[3], § 1 International Private Law Act, margin number 12; *Jud/Aspöck*, Internationales Privatrecht; p. 14;) contradictions of norms are to be remedied by adjustment ("harmonisation"). Adjustment implies that parts of the law are not applied or, if necessary, amended inasmuch as this is needed to resolve the conflict. Harmonisation would mean to follow the "least possible sacrifice" principle and to interfere with the applicable law as little as possible.

210. In the case at hand, assignability under California law must be assumed so as to reach a harmonisation without having to interfere with Austrian procedural law (held also by the Austrian Supreme Court in 3Ob189/12h on a conflict between Croatian substantive law and Austrian civil procedural law).

211. As an aside it should be noted that the prohibition of assignment which Defendant has stipulated in section 19.1 [TN9] of its Statement of Rights and Responsibilities (Enclosure ./A) is not applicable to torts under Californian law, since they do not constitute a contractual claim but a claim in tort. The prohibition of assignment however only relates to "rights (…) under this Statement" and - even by its wording - not to claims which, under the law chosen by Defendant, specifically do not arise from the contract. The Statement of Rights and Responsibilities must at any rate be interpreted in the interest of the consumer (cf. Article 5 of directive 93/12/EEC).

212. Ultimately, the application of Austrian overriding mandatory rules would lead to the same result: The prohibition of assignment agreed by way of a choice of law in general terms and conditions in order to prevent a "class action under Austrian law" vis-à-vis consumers, would clearly be *contra bonos mores* within the meaning of section 879 *ABGB* (General Civil Code). Since section 879 *ABGB* is an overriding mandatory rule (cf. Article 6(2) of directive 93/13/EEC), non-national law is not to be applied to *contra bonos mores* issues.

C. Claims assigned by a German user

213. Another user of Defendant's services having his place of residence in Germany has assigned his claim arising out the infringements committed against him to Plaintiff (see Enclosure ./AC). By virtue of Defendant's choice of law, German law applies to agreements with German users (see 17.3 in Enclosure ./A).

214. The notion of immaterial damages is inexistent in German law if the right to data protection is violated by private persons pursuant to section 7 *BDSG* (*German Federal Data Protection Act).* Immaterial damages must however be awarded in the case of violation of a – materially overlapping – general personality right (section 823 *BGB* (German General Civil Code) in conjunction with Article 1 and Article 2 *GG (Grundgesetz*, Basic Law) and the case law of the German Federal Constitutional Court on the right to informational self-determination). The unauthorized, wilful, systematic, secret, and comprehensive, at any rate wrongful processing of personal data out of base motives (in particular the commercialisation of the personality, profit maximisation and supporting the intelligence operations of a third country) constitutes a serious violation.

215. Alternatively, Plaintiff also bases the claims assigned by the German user again on the direct applicability of Article 23 of directive 95/46/EC, which does not limit compensation for immaterial damage. For reasons of procedural caution, these claims, too, have been quantified – subject to further extension – at EUR 500, plus the claim to profitable utilization to be determined.

216. Ultimately, German law on enrichment provides in sections 812 et seq. *BGB* (German General Civil Code) that advantages gained from the wrongful interference with third-party rights must be compensated. Defendant has drawn financial advantages from this interference. The advantage gained therefore must be rescinded under enrichment law. On the amount of such advantage, reference is made to the arguments set out under margin numbers 193, 194.

Evidence: As before

If contested, submission of further documents.

Submission of further evidence reserved.

C. Claim to submission of a statement of account

217. The enriched person owes the harmed person the surrender of the advantage gained, or at least the payment of a reasonable usage fee, in the case of mere use. In order to ascertain the advantage gained, established doctrine and case law affirm a claim to the submission of a statement of account (cf. *Rummel, ABGB*², margin number 18 on section 1041 *ABGB*). Plaintiff also has a right to being submitted a statement of account as regards the advantages which Defendant gained from the wrongful use and exploitation of his own data, as well as of the data of those persons who assigned their claims to compensation to Plaintiff.

D. Other original claims of Plaintiff

218. Regarding Defendant's infringements set out under II., Plaintiff has a number of other claims vis-à-vis Defendant for declaratory statement and injunctive relief (irrespective of fault), elimination and deletion, in addition to the claims to compensation and on account of unjust enrichment already addressed. Moreover, Plaintiff also has a right to information (cf. II. K.)

219. These claims are based on the provisions referred to above, alternatively on any conceivable legal base.

V. Admissibility of the Statement of Claim

A. Admissibility of a "class action under Austrian law"

220. The Austrian Supreme Court has held that "class actions under Austrian law" as an objective accumulation of actions according to section 227 para 1 *ZPO* (Code of Civil Procedure) are admissible if there is a "relevant common basis" and essentially the same questions of fact and of law are to be assessed in the main issue (cf. 4Ob116/05w and 6Ob224/12b and RS0037628). This requirement is satisfied, since the assigned claims are - factually and legally - fully identical with Plaintiff's original financial claims. Only for German users, the claims which result from the very same questions of fact and of law must be assessed according to German law.

221. Thus, the claims assigned to Plaintiff can be enforced by way of legal action together with his original claims (section 227 para 1 *ZPO*, Code of Civil Procedure); according to the Supreme Court's case law, the original and assigned claims may also be jointly heard (beyond what is stipulated in section 227 *ZPO*).

B. Admissibility of legal action

222. Unlike other fundamental rights, the right to data protection has a direct third-party effect vis-à-vis private persons (cf. e.g. *Dohr/Pollirer/Weiss/Knyrim*, Datenschutzrecht, § 1, note 2;) and is therefore a matter of civil law within the meaning of section 1 JN (*Jurisdiktionsnorm*, Law on the jurisdiction of Austrian courts in civil matters).

223. By virtue of explicit European law provisions set out in Article 22 of directive 95/46/EC, the data subject may therefore take recourse to civil law action (to the same effect also e.g. section 32 *DSG*, Austrian Data Protection Act). This possibility of redress and enforcement is explicitly independent of any administrative proceedings which may have been instituted.

VI. Jurisdiction of the seized court

A. Local jurisdiction regarding Plaintiff's original claims

224. Pursuant to Article 16(1) of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, the Court has jurisdiction at any rate.

225. This is not changed by Defendant's choice of jurisdiction in its Statement of Rights and Responsibilities (which according to section 16.1 of the Statement of Rights and Responsibilities Enclosure ./A, wants courts in California to have jurisdiction), since this clause is at any rate invalid vis-à-vis a consumers according to Article 17 of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

226. Moreover, this choice would probably be invalid even under Californian *forum-non-conveniens* rules. Besides, a U.S. judgment would not be recognized in Ireland and therefore not enforceable vis-à-vis Defendant in Ireland, which is why Defendant's choice of jurisdiction is not only invalid but also impractical.

B. Local jurisdiction regarding the assigned claims

227. The above applies without distinction to the claims assigned by other users. The claims assigned all originate from consumers within the meaning of Article 15(1) of Council Regulation (EC) No 44/2001 which have entered into a contract of identical wording as Plaintiff with Defendant. Defendant has targeted its activities to the states of residence of these consumers without distinction.

228. Plaintiff is not seeking any profits from asserting these claims. Accordingly, Plaintiff has agreed by way of contractual assignment (Enclosure ./AC) to pass on any advantages gained (deducting costs which may be incurred) to the assignors. With Plaintiff being a natural person who does in no way act with entrepreneurial intent, the case law of the CJEU in C-89/91 (on assignors acting in pursuance of their business) and C-167/00 (on consumer associations) is irrelevant.

229. Therefore, the court has jurisdiction also for the claims assigned to Plaintiff pursuant to Articles 15 and 16 of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Assumedly, the Supreme Court also based itself on this view in 10 Nd 510/00. Established doctrine concurs (e.g. *Simotta* in Fasching, Zivilprozessgesetze, Art 15, margin number 109, with further references; *Nemeth* in *Burgstaller/ Neumayr/Geroldinger/Schmaranzer,* Internationales Zivilverfahrensrecht, Art 15, margin number 19, with further references; *Schlosser,* EU-ZPR, Art 15 Rome Convention, margin number 3; *Geimer/Schützer*, Europäisches Zivilverfahrensrecht, Art 15, margin number 19, with further references; and many others).

Evidence: As before

If contested, submission of further documents

Submission of further evidence reserved.

C. Subject-matter jurisdiction

230. The court's subject-matter jurisdiction results from the special jurisdiction pursuant to section 32(4) *DSG* (Austrian Data Protection Act) for data protection matters in conjunction with sections 49, 50 and 51 para 1 subpara 1 JN (*Jurisdiktionsnorm*, Law governing the jurisdiction of Austrian courts) and from the fact that Defendant is a company registered in the companies register of the Republic of Ireland.

231. Jurisdiction equally results from the monetary value of Plaintiff's claims and from the assessment of the personal performances and omissions according to section 59 JN.

VII. Prayer for relief

Since Defendant is unwilling to desist from the outlined infringements and to provide the requested information, in spite of having been requested several times by Plaintiff, continues harming Plaintiff and the assignors and/or unjustly enriching itself by the wrongful use of data, Plaintiff is forced to bring this action. For the reasons set out in detail in the narrative of the claim, and basing himself on any and every conceivable legal ground, Plaintiff is seeking the following

J U D G M E N T

[B. ROLES and C. RESPONSIBILITIES]

1. For a declaration with effect between Plaintiff and Defendant that Plaintiff is the "*Auftraggeber*/controller" within the meaning of section 4 para 4 *DSG*, Austrian Data Protection Act, (corresponding to the "controller" in Article 2(d) of directive 95/46/EC and the "data controller" in s 1(1) DPA, Irish Data Protection Act) of the data applications operated via the *facebook.com* portal for his personal purposes (in particular his timeline, updates, events, photos, videos, groups, pages and personal messages, friends lists and applications), whereas Defendant in this respect only acts as a "*Dienstleisterin*/ processor" within the meaning of section 4 para 5 *DSG* (corresponding to the "processor" in Article 2(e) of directive RL 95/46/EG and the "data processor" in s 1(1) DPA).

2. For a declaration with effect between Plaintiff and Defendant that Defendant is the "*Auftraggeber*/controller" within the meaning of section 4 para 4 *DSG*, Austrian Data Protection Act, (corresponding to the "controller" in Article 2 (d) of directive 95/46/EC and the "data controller" in s 1(1) DPA, Irish Data Protection Act) of the data applications operated for its own purposes on the *facebook.com* portal (in particular the compilation and aggregation of contents, the search function, advertising, user administration and similar data applications).

3. Defendant is liable to henceforth use data of Plaintiff which he himself stores and transmits via the *facebook.com* portal for his personal purposes (in particular his timeline, updates, events, photos, videos, groups, pages and personal messages, friends lists and applications) and in respect of which he himself is the "controller" and Defendant merely the "processor" only according to Plaintiff's instruction and shall cease and desist using these data contrary to Plaintiff's instructions.

4. Defendant is liable to amend the Statements of Rights and Responsibilities, Enclosure ./A and the Data Use Policy, Enclosure ./C in a manner so that the controller for each and every data application (in particular timeline, updates, events, photos, videos, groups, pages, personal messages, friends lists, applications, compilation and aggregation of contents, search function, advertising, user administration) is clearly specified, and to change the software provided so that Plaintiff can meet his duties arising from section 6

para 2 and section 10 *DSG,* Austrian Data Protection Act (corresponding to Article 17(2) to (4) of directive 95/46/EC): specifically, arrangements shall be made so that the data are processed according to Plaintiff's instructions and that Plaintiff can effectively give such instructions (e.g. by options for an automatic and/or simple deletion and administration of individual data, entire data categories and parts thereof which can be meaningfully selected).

4.1. *In eventu,* for a declaration with effect between Plaintiff and Defendant that the existing agreements between Plaintiff and Defendant (in particular the Statement of Rights and Responsibilities, Enclosure ./A and the Data Use Policy, Enclosure ./C) do not satisfy the requirements of section 10 para 1 *DSG*, Austrian Data Protection Act (and/or of Article 17 (2) to (4) of directive 95/46/EC).

5. For a declaration with effect between Plaintiff and Defendant that Defendant must ensure the security of Plaintiff's data being used within the meaning of s 2(1)(d), 2(2) in conjunction with 2C(2) DPA (and/or of Article 17 of directive 95/46/EC, corresponding to section 14 *DSG*, Austrian Data Protection Act).

6. For a declaration with effect between Plaintiff and Defendant that section 3, first sentence, *"We do our best to keep Facebook safe, but we cannot guarantee it"*, the entire section 16.3 of the Statement of Rights and Responsibilities, Enclosure ./A, and the sentence *"We try to keep Facebook up, bug-free and safe, but can't make guarantees about any part of our services and products"* under the heading *"Security and bugs"* in the Data Use Policy, Enclosure ./C are ineffective.

[D. and E. GENERAL CONSENT, USE OF DATA]

7. For a declaration with effect between Plaintiff and Defendant that Plaintiff's consent to the Statement of Rights and Responsibilities, Enclosure ./A and to the Data Use Policy, Enclosure ./C in the present form does not authorise Defendant to use Plaintiff's data for its own purposes (in particular advertising, data aggregation and analysis).

8. Defendant shall henceforth cease and desist using any of Plaintiff's data for its own purposes (in particular advertising, data aggregation and analysis) invoking the Statement of Rights and Responsibilities, Enclosure ./A and the Data Use Policy, Enclosure ./C and Plaintiff's supposedly inferable "consent", or any equally vague terms and conditions to the same effect, non-exhaustive enumerations, general clauses and "third-party consents", or similar.

9. For a declaration with effect between Plaintiff and Defendant that the "consent by third parties" presumed by Defendant as well as the "ex-ante consent" by Plaintiff equally presumed by Defendant to the recording, provision and transmission of his data by third parties without knowledge of the specific case (e.g. a specific photo or update) are ineffective.

[F. SOCIAL PLUG-INS]

10. Defendant shall henceforth cease and desist using Plaintiff's data concerning the visit and/or use of third-party sites (in particular by using social plug-ins and similar techniques), unless technical data are solely processed for the purpose of displaying website elements, and unless Plaintiff has given his ex-ante consent to the specific processing without any doubt, freely, informed and unequivocally ("opt-in"; e.g. by clicking on a social plug-in).

[G. BIG DATA]

11. Defendant shall henceforth cease and desist interconnecting Plaintiff's data with data from third-party sources (e.g. from other users or external companies) or using similar techniques for its own commercial purposes (in particular for advertising, data aggregation and analysis), unless Plaintiff has given his ex-ante consent to the specific processing without any doubt, freely, informed and unequivocally ("opt-in").

12. Defendant shall henceforth cease and desist creating new data by extrapolating and analysing Plaintiff's data and using similar techniques for its own commercial purposes (in particular advertising, data aggregation and analysis), unless Plaintiff has given his ex-ante consent to the specific processing without any doubt, freely, informed and unequivocally ("opt-in").

13. Defendant shall henceforth cease and desist using Plaintiff's data for its own commercial purposes (in particular advertising, data aggregation and analysis) invoking any other legitimate reasons than Plaintiff's consent after a reasonable period, no later than 90 days at the latest, unless these are statistical master data (e.g. age, gender or place of living).

[H. GRAPH SEARCH]

14. Defendant shall henceforth cease and desist using Plaintiff's data in the Graph Search data application and by similar techniques, unless Plaintiff has given his ex-ante consent without doubt, freely, informed and unequivocally ("opt-in").

[H. APPS]

15. Defendant shall henceforth cease and desist using and transmitting Plaintiff's data for "external applications" and for similar systems used by other users.

[J. PRISM]

16. Defendant shall henceforth cease and desist having Plaintiff's data processed and used by processors which do not provide a guarantee against mass surveillance by a third country (in particular by its parent company *Facebook Inc*. in the United States of America).

[K. PROVISION OF INFORMATION]

17. Defendant is liable to provide to Plaintiff within fourteen days full information in writing and free of charge about all personal data of Plaintiff it processed, stating the precise purpose and whenever possible, the exact origin and specific recipient of the data, as appropriate, failing which enforcement proceedings shall be instituted.

[D. to J. DAMAGES, ENRICHMENT]

18. Defendant is liable to pay to Plaintiff an amount of EUR 4000 within fourteen days to the account of his legal counsel, failing which enforcement proceedings will be instituted.

19. Defendant is liable to submit to Plaintiff within fourteen days a statement of account on the wrongful use and exploitation of Plaintiff's data and of the data of the assignors [redacted] failing which enforcement proceedings shall be instituted.

20. Defendant is furthermore liable to pay to Plaintiff within fourteen days the full amount of the credit shown in the statement of account, with the actual amount of the sought payment remaining reserved until a statement of account has been submitted according to paragraph 18 of the sought judgment, failing which enforcement proceedings shall be instituted.

[LITIGATION COSTS]

21. Defendant if further liable to reimburse Plaintiff for the costs of litigation pursuant to section 19a *RAO* (Code of the Austrian Bar Association) through payment to his legal counsel within fourteen days, failing which enforcement proceedings shall be instituted.

Maximilian Schrems

Costs incurred:

Statement of claim, rate item 3A	729.50 EUR
Assessment base 40,000 EUR	
100 % unit rate	729.50 EUR
Total costs	1,459.00 EUR
Electronic filing fee	3.60 EUR
Subtotal	1,462.60 EUR
20% VAT of 1,462.60 EUR	292.52 EUR
Total	1,755.12 EUR
Lump-sum fees	1,389.00 EUR
Grand total	3,144.12 EUR

Translator's notes:

TN1: should correctly read Art 15(1) point (c)

TN2: should correctly read Directive 95/46/EC

TN3: should correctly read Article 3 (2) directive 95/46/EC

TN4: should correctly read Article 17 (3), second indent

TN5: should correctly read Article 8(2) point (a) of directive 95/46/EC

TN6: German should read Datenverwendungsrichtlinien (Data Use Policy) not *Datenschutz-richtlinien* (data protection regulations)

TN7: should read correctly in German Beklagte (Defendant) instead of Betroffene (person concerned, also data subject)

TN8: should correctly read 2(1)(b)(iii) DPA

TN9: should correctly read 19.6

English Translation of German Original

Die genaue Übereinstimmung d. vorstehenden
Übersetzung mit der/dem

angehefteten – vorliegenden – beglaubigten- Original – Abschrift bzw. Ablichtung

bestätige ich unter Berufung auf meinen Eid.

Mag. Michaela Spracklin
Allgemein beeidete und gerichtlich zertifizierte Dolmetscherin für die englische Sprache

Wien, am 30. September 2014

Upon the authority of my oath I herewith confirm
the precise correspondence of the English translation
with the attached – submitted – certified original – copy /photocopy
of the original German document.

Michaela Spracklin
Sworn and court-certified interpreter for English

Vienna, 30 September 2014

English Translation of German Original