

# Facebook's Real Name Policy

## Bye-Bye, Max Mustermann?

by **Sandra Schmitz**, Ass. iur. LL.M, Ph.D. candidate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg.

**Abstract:** Facebook requires all members to use their real names and email addresses when joining the social network. Not only does the policy seem to be difficult to enforce (as the prevalence of accounts with people's pets or fake names suggests), but it may also interfere with European (and, in particular, German) data protection laws. A German Data Protection Commissioner recently took action and ordered that Facebook permit pseudonymous accounts as its current anti-pseudonymous policy violates § 13 VI of the German Telemedia Act. This provision requires telemedia providers to allow for an anonymous or pseudonymous use of services inso-

far as this is reasonable and technically feasible. Irrespective of whether the pseudonymous use of Facebook is reasonable, the case can be narrowed down to one single question: Does German data protection law apply to Facebook? In that respect, this paper analyses the current Facebook dispute, in particular in relation to who controls the processing of personal data of Facebook users in Germany. It also briefly discusses whether a real name policy really presents a fix for anti-normative and anti-social behaviour on the Internet.

**Keywords:** Facebook, Real Names, Data Protection, Personal Data, Germany

© 2013 Sandra Schmitz

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Sandra Schmitz, Facebook's Real Name Policy: Bye-Bye, Max Mustermann?, 4 (2013) JIPITEC 3, 190

## A. Introduction

1 One of the appealing integral characteristics of the Internet is anonymity, meaning the ability to conceal one's identity while communicating.<sup>1</sup> The real author of a message is then not identifiable. In this context, if we speak of anonymity, this also encompasses the use of pseudonyms. On the Internet, users often use screen names, i.e. pseudonyms, when they post messages, chat or are otherwise communicating. The advantage of using a pseudonym instead of remaining completely anonymous is that while concealing one's real identity, it is possible for third parties to recognise that different messages are written by the same author. Pseudonyms allow the allocation of postings to a specific user whose real name is not known to the public. Even where real identity

becomes important for the recipients of the communication – for example, on online auction sites like eBay – the real identities of users are not revealed to the general public. Only where a contract of sale is established will the anonymity of seller and buyer be lifted to allow the performance of the sales contract. Of course, there are also online transactions that require a priori real identity verification, such as banking transactions, for example. However, recently Internet service providers like Google (in relation to their Google+ service) and Facebook have forbidden the use of pseudonyms, demanding from members that their online identity be the same as in the offline world.<sup>2</sup> More than the world's largest social network, Facebook in particular is a huge data-mining machine capturing and processing every click and interaction on its platform. Obviously,

the harvested data becomes more valuable if it can be linked to real persons with real names. Hence, it is no surprise that Facebook vigorously advocates the use of real names in the online world. Officially, they do so in the interest of their users, arguing that a real name policy may serve as a fix for bad behaviour, in particular cyberbullying, trolls and illegal activities. The underlying assumption in this respect is that users will refrain from anti-social and anti-normative behaviour if their name is attached to a posting.

- 2 It is not surprising that Facebook appealed orders by a German data protection authority which required Facebook to allow pseudonyms on user profiles. Under German law, telemedia service providers are obliged to allow the pseudonymous or anonymous use of their service as long as this is reasonable and technically feasible. While primarily the question of the legitimacy of the mandatory real name policy was in the public eye, the court did not discuss this question in detail as the outcome of the case depended on one single question: Does Facebook have to respect German data protection law? This would be the case if German data protection applied to Facebook. The whole discussion thus centres around the basic question of applicable law for a globally active service provider.
- 3 In order to answer this question, it is crucial to determine whether there has been a valid choice of German law, and to determine where and by whom data is being processed. In the following, this paper will look into Facebook's corporate structure and its terms of use before focussing on the order of the German data protection authority and the subsequent court proceedings.

## 1. The corporate structure of Facebook and its terms of use

- 4 While Facebook users in general use the notion "Facebook" interchangeably for the service and the service provider, it is important to know that there is not one single Facebook company. Though most official statements of Facebook spokespersons also just refer to Facebook as such, for the determination of applicable law it is of fundamental importance to distinguish between the global player Facebook Inc., its European subsidiary Facebook Ireland Ltd. and further smaller Facebook subsidiaries which are all in some way involved in providing and/or administering the platform Facebook.<sup>3</sup> As the major part of the lawsuits deal with the relation of Facebook Inc. towards Facebook Ireland Ltd., it is necessary to have a basic understanding of the corporate structure of Facebook and its rules on jurisdiction and applicable law.

## 1. Corporate structure of Facebook

- 5 Facebook, which was founded in 2004, is operated by Facebook Inc., a US multinational Internet corporation. Facebook has its key assets, its headquarters and the site of its corporation in the US.
- 6 In 2008, Facebook established its European headquarters in Dublin. The role and position of the Irish subsidiary, Facebook Ireland Ltd., in relation to users from outside the US and Canada was enhanced in 2010 when Facebook's Statement of Rights and Responsibilities was amended to set forth that these users have contracts with Facebook Ireland Ltd. and not Facebook Inc.<sup>4</sup> With Facebook Ireland Ltd. being in charge of all users outside the US and Canada, Facebook avoids material jurisdiction for corporation tax on all international revenue in the US.<sup>5</sup> Beside Facebook Ireland Ltd., there are four additional subsidiaries in Ireland: Facebook Ireland Holdings; Facebook International Holdings I; Facebook International Holdings II; and Facebook Payments International Ltd. In Germany, Facebook seems to have only one local subsidiary, Facebook Germany GmbH, which is in charge of marketing and acquisition for the local market.

## 2. Facebook's rules on jurisdiction and choice of law

- 7 Facebook's terms of use are entitled "Statement of Rights and Responsibilities". The Statement constitutes Facebook's terms of service that "govern (Facebook's) relationship with users and others that interact with Facebook".<sup>6</sup> Users "agree" to these terms by simply using or accessing Facebook.<sup>7</sup>
- 8 The Statement also contains a choice-of-law clause. Section 16.1. provides that "any claim, cause of action or dispute (claim) [a user has with Facebook] ... arising out of or relating to the Statement or Facebook" will be resolved:
 

*Exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.*
- 9 In accordance with the Statement, users will thus have to resolve disputes with Facebook in California under Californian law, even if they are from outside the United States.<sup>8</sup>
- 10 However, for users in Germany, section 17.3 of the Statement<sup>9</sup> exclusively provides that section 16.1 is replaced by the following clause:

*“This Statement is subject to German law”.*<sup>10</sup>

- 11 In relation to data protection rules, the current data policy, last updated on 11 December 2012, states that Facebook Ireland Ltd. is the data controller responsible for the personal information of users from outside the US and Canada.<sup>11</sup>

## II. Facebook’s real name policy

- 12 Browsing Facebook, users were likely to meet Max Mustermann<sup>12</sup> or variations thereof as well as numerous teenage girls with the last name “Bieber”.<sup>13</sup> While Max Mustermann, which might easily be identified as a fake name, has lately disappeared from Facebook, users are turning to much subtler tricks to avoid being banned from Facebook: they may use a middle name as a last name, turn to a fictional character’s name, invent a real-sounding name, borrow their mother’s maiden name or a common last name, an abbreviation, or other pseudonyms that equally violate Facebook’s real name policy. This mandatory real name policy is enshrined in Facebook’s community standards and requires all users to use their real identities including their real names on Facebook:

*- The name you use should be your real name as it would be listed on your credit card, student ID, etc.*

- Nicknames can be used as a first or middle name if they’re a variation of your real first or last name (like Bob instead of Robert)
  - You can also list another name on your account (ex: maiden name, nickname, or professional name), by adding an alternate name to your timeline
  - Only one person’s name should be listed on the account – timelines are for individual use only
  - Pretending to be anything or anyone is not allowed.<sup>14</sup>
- 13 Facebook often emphasises that Facebook is for real people using their real identities. According to the community standards, real identities and real names are required to keep the social network “safe” and guarantee that users know whom they are connecting with.<sup>15</sup>
- 14 For those who want to represent a business, brand or even a pet, Facebook allows the creation of a so-called “Facebook page”.<sup>16</sup> In addition, users may also list their professional title as an alternate name on their personal timelines. However, this still meant that Stefani Germanotta could not run her Facebook profile under her stage name Lady Gaga.<sup>17</sup> In a bid to attract more celebrities, which in turn may attract more users, Facebook slightly diluted its strict application of the real name policy and now allows celebrities – following a verification of their identity – to use their well-established stage names on their per-

sonal accounts.<sup>18</sup> However, they need to include their real name in the information section of the profile. In order to guarantee that only “real” celebrities make use of this exception, a user will need at least 20,000 subscribers to be allowed to benefit from this new pseudonym privilege. Ultimately, Facebook relies on the honesty of its customers, as from a technological perspective anyone can still open an account under a false identity or pseudonym.

## III. The right to pseudonymous use of media services under German law

- 15 In general, users in Germany have a *per se* reasonable expectation of privacy with respect to the revelation of their identity to the general public.<sup>19</sup>
- 16 A unique feature of the German law on Internet services is that the possibility of anonymous or pseudonymous use of Internet services is prescribed by law. § 13 VI of the Telemedia Act of 2007 (TMG) foresees the anonymous or pseudonymous use of Internet services as well as the anonymous or pseudonymous payment of these services. The wording of § 13 VI TMG is as follows: “The service provider must allow the anonymous or pseudonymous use of telemedia services and their payment, insofar as this is technically feasible and reasonable. The user must be informed about this possibility.”<sup>20</sup>
- 17 This is not a novel principle in German law. Even the predecessors of the TMG, the Teleservices Data Protection Act, which came into force on 1 January 2000, and the State Treaty on Media Services, which came into force 1 August 1997, contained identical provisions.<sup>21</sup>
- 18 § 3 VI a of the Federal Data Protection Act (BDSG<sup>22</sup>) defines “rendering pseudonymous” as meaning replacing the data subject’s name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject.<sup>23</sup>
- 19 The provision recognises that the success of the Internet is inter alia based on the possibility of the anonymous use.<sup>24</sup> The anonymous as well as the pseudonymous use follows the basic principle of data reduction and data economy, meaning that as little personal data as possible shall be collected, processed and used.<sup>25</sup> The principle of data reduction and data economy can also be found in Article 6 I c) and e) as well as in Recital 46 of the EU Data Protection Directive.<sup>26</sup> This principle is explicitly set forth in § 3a BDSG<sup>27</sup> and also derives from the constitutional right to informational self-determination.<sup>28</sup> Under the right to informational self-determination, every individual is in principle entitled to determine the disclosure and use of his/her personal data.<sup>29</sup> If

individuals are not sure whether dissenting behaviour is noticed and whether information is permanently stored, used and passed on, they may try to avoid dissenting behaviour in order to not attract attention. This may even result in abstaining from making use of their basic human rights.<sup>30</sup> The purpose of § 13 VI TMG is to avoid the generation of personal data right from the start.<sup>31</sup>

- 20 Allowing a user the anonymous or pseudonymous use of telemedia services does not mean that the user has a right to stay anonymous in front of the service provider.<sup>32</sup> There is no right to an anonymous or pseudonymous contractual relationship.<sup>33</sup> This means that while users are entitled to use a screen name, this does not exclude the possibility of the telemedia service provider asking for the user's real identity in their internal relationship.
- 21 Even in Germany, the right to anonymous or pseudonymous use is not granted without limits. The right finds its limits where the granting of anonymous or pseudonymous use would be unreasonable for the service provider.<sup>34</sup>
- 22 What is important to keep in mind is that § 13 VI TMG only concerns the possibility of anonymous or pseudonymous use and does not prohibit disclosure orders against Internet service providers by injured parties. In simple terms, the provision only prohibits service providers to ask for a user's real name and display his real name when it is not necessary to do so.

## B. ULD v. Facebook

- 23 When Facebook took rigorous steps against some German users who had not obeyed its real name policy by suspending their accounts, the Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein<sup>35</sup> took action against Facebook. Schleswig-Holstein's Privacy Commissioner and Head of ULD, Thilo Weichert, announced that it cannot be accepted "that a U.S. portal like Facebook violates German data protection law unopposed and with no prospect of an end".<sup>36</sup> However, Facebook only violates German data protection law if § 13 VI TMG constitutes a data protection norm, and if German data protection law applies to Facebook. With regard to the applicable law, the determining factor is the location of the data controller of Facebook's user data. Only where the data controller is located in Germany, or is not located on Community territory at all, must German data protection law be obeyed. With regard to the latter, Article 4 I c) Data Protection Directive foresees the application of national law, where the data controller is not located on Community territory, whereas if the data controller has an establishment in another EU Member State, Article 4 I a) prescribes the application of the

law of this EU Member State. Hence, the whole case centred around the debate on which of Facebook's companies does what and where.

## I. The administrative proceedings

- 24 As a first step, the ULD issued administrative orders against Facebook Inc. and Facebook Ireland Ltd. to refrain from enforcing the real name policy in relation to users in Schleswig-Holstein and allow pseudonymous accounts as required by the TMG.<sup>37</sup>

### 1. The orders of the ULD

- 25 The orders of 14 December 2012 stipulated that Facebook Inc. as well as Facebook Ireland Ltd. would be fined 20,000 euro if they did not comply with the orders within two weeks.<sup>38</sup> In German administrative law, the effect of any decision is immediate when notified. The ULD also ordered that an appeal would not have suspensory effect, meaning that Facebook had to implement the ordered measures irrespective of an appeal. Hence, Facebook was obliged to allow users from the German state of Schleswig-Holstein (for which the ULD has competence) to use pseudonyms immediately.
- 26 With regard to Facebook's real name policy, the ULD found the policy to be in violation of § 13 VI TMG. The decision and orders issued by ULD can be summarized as follows:
  - The permission to use pseudonyms on Facebook is reasonable. The real name obligation neither prevents abuse of the service for insults or provocations nor does it help prevent identity theft. Against this other precautions are necessary.
  - To ensure the data subjects' rights and data protection law in general, the real name obligation must be immediately abandoned by Facebook.
- 27 Orders were issued to both companies, Facebook Ireland Ltd. and Facebook Inc., as they were found to be joint data controllers. Although all Facebook users from outside the US and Canada have contracts with Facebook's Irish subsidiary Facebook Ireland Ltd., the ULD concluded that, as regards the real name policy, Facebook Inc. and Facebook Ireland Ltd. were jointly responsible in legal terms.<sup>39</sup> Nevertheless, the ULD applied § 1 V 2 BDSG, which transposes Article 4 I c) Data Protection Directive into national law. Under this provision, German law is applicable if a data controller who collects, processes or uses personal data inside Germany is not located in an EU or EEA Member State.<sup>40</sup> Although Facebook Ireland Ltd. is located in a Member State, the ULD found that it only played a rather subordinate role in the data

processing, while from an objective point of view, the actual control over the data and all authority in terms of purposes and means of processing remained with Facebook Inc.<sup>41</sup> Hence, Facebook was ordered to observe German data protection laws, and in particular § 13 VI TMG, in relation to Facebook users in Germany.

## 2. The ULD's reasoning

28 In the proceedings following Facebook's appeal, the ULD specified its position and provided further arguments supporting its claim. These arguments are well worth mentioning as they also deal with the role of Facebook Germany GmbH.

### a.) The ULD's reasoning in relation to Facebook Inc. USA

29 According to the ULD, Facebook Inc. collects, processes and uses personal data in the meaning of § 3 VII BDSG, Article 2 d) Data Protection Directive: During the registration process on www.facebook.com, Facebook Inc. collects personal data; in addition, Facebook Inc. installs cookies on the computers of its users when they access the website. All data that is collected is stored and processed on servers of Facebook Inc., which are currently all situated in data centres in the US.<sup>42</sup>

30 Thus, the ULD was not satisfied that Facebook Ireland Ltd. was processing personal data in the context of its own activities.<sup>43</sup> It is not sufficient to just hold an office in a Member State while the business policy is exclusively determined by a company in the US.<sup>44</sup> Moreover, Facebook Inc. is factually in charge of the data processing as it has the authority to determine the purposes and means of processing. The notion of context of activities in Article 4 I a) Data Protection Directive, however, requires more than the existence of a mere establishment, namely the active involvement in activities relating to personal data processing.<sup>45</sup> Pursuant to Article 2 b) Data Protection Directive, processing of personal data shall mean

*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

31 In this regard the degree of involvement of the establishment in the activities in the context of which personal data are processed is crucial.<sup>46</sup> The question is "who is doing what": only where an establishment processes personal data in the context of its own activities will the applicable law be that of the place of establishment. The ULD was not convinced that

Facebook Ireland Ltd. carries out the processing of the relevant user data in the context of the activities of an establishment of Facebook Inc. in Ireland, nor does Facebook Ireland Ltd. instruct Facebook Inc. to process the relevant data.<sup>47</sup> As regards the latter, Facebook Ireland Ltd. did not provide evidence of contractual agreements that determine inter alia the purpose of processing of personal data, the types of personal data, the technical-organisational data security measures, and details about controls of Facebook Ireland Ltd.<sup>48</sup> Article 17 III Data Protection Directive requires the existence of a contract or legal act binding the processor to the controller and stipulating in particular that "the processor shall act only on instructions from the controller".

32 In consideration of the registration process on www.facebook.com where Facebook Inc. collects personal data and makes use of automated equipment (the users' computers) by installing cookies on these as well as using equipment in Germany via the content delivery network Akamai,<sup>49</sup> the ULD concluded that German national law has to be applied in relation to Facebook users in Germany in accordance with Article 4 I c) Data Protection Directive (data controller of personal data outside the EU/EEA, which makes use of equipment situated on German territory).

### b.) The ULD's reasoning in relation to Facebook Ireland Ltd.

33 Facebook Ireland Ltd. qualified as a controller in the sense of § 3 VII BDSG and Article 2 d) Data Protection Directive when it collects, processes and uses personal data in relation to the blocking of accounts and asking users to utilise their real names.<sup>50</sup> Further objective control of data processing could not be established.

34 The application of German law to Facebook Ireland Ltd. was also based on the role of Facebook Germany GmbH.<sup>51</sup> According to the ULD, Facebook Germany GmbH is an establishment of Facebook Inc. in Germany. This was based on the assumption that the role of Facebook Germany GmbH goes beyond marketing and acquisition for the local market as it is also a communication channel for Facebook Ireland Ltd. and Facebook Inc.<sup>52</sup> The Irish Data Protection Commissioner had received copies of data-processing contracts entered into by Facebook Ireland Ltd. as data controller and inter alia Facebook Germany.<sup>53</sup> Unfortunately, the ULD had no knowledge of the content of these contracts, but the mere existence was used as an indication that Facebook Germany is also involved in data processing. Accordingly, the ULD concluded that the controller of personal data (Facebook Inc.) is established on the territory of several Member States (here: Ireland and Germany), and thus, pursuant to Article 4 I a) Data Protection Di-

rective, must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable. Hence, the services offered on [www.facebook.com](http://www.facebook.com) must comply with German data protection law.

### c.) The ULD's determination of joint control

35 Although the ULD could not be convinced that Facebook Ireland Ltd. is the sole data controller for personal data of European users, it was satisfied that Facebook Ireland Ltd. and Facebook Inc. USA control the data jointly.<sup>54</sup> Joint control in the context of Article 2 d) Data Protection Directive does not require that all controllers equally determine and are equally responsible for a single processing operation; "jointly" rather needs to be interpreted as meaning "together with" or "not alone".<sup>55</sup> In case of several actors, they may have a very close relationship (sharing, for example, all purposes and means of processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof).<sup>56</sup>

### d.) Choice-of-law clause

36 The ULD also argued that the application of German data protection law is supported by the "Statement of Rights and Responsibilities" of Facebook, section 16.1., which provides that the Statement is subject to German law.

### e.) The ULD's conclusion: applicability of § 13 VI TMG

37 As Facebook Inc. and Facebook Ireland Ltd. were both considered providers of telemedia services,<sup>57</sup> they were obliged to allow the pseudonymous use of the social network insofar as this is technically feasible and reasonable. The registration procedure at [www.facebook.com](http://www.facebook.com) which requires users to enter their real name, and the blocking of users who did not register under their real name, violates § 13 VI TMG.<sup>58</sup>

38 When examining whether there are legally permissible, less restrictive means which could lead to equivalent results, the ULD stressed that Facebook basically has a monopoly when it comes to social networks; in particular, communication of minors in many regards (e.g. spare time activities) takes place only on Facebook.<sup>59</sup> Hence, the ULD established a certain necessity of users to register on Facebook and, subsequently, to give up privacy.<sup>60</sup> The ordered measures were thus considered reasonable, even in light of the competing interests of Facebook at hand. Facebook's freedom to conduct their busi-

ness model as well as its obligations under §§ 7 – 10 TMG (transposing Article 12-15 E-Commerce Directive<sup>61</sup> into national law) did not outweigh the interests of the users.<sup>62</sup>

## 3. The position of Facebook

39 As mentioned above, the discussion of which data protection regime has to be applied to German Facebook users can be narrowed down to one single question: Who is the data controller of the personal data of Facebook's users? According to Facebook, the answer to that question is clear: the data controller of the personal data of European users is Facebook Ireland Ltd. and not Facebook Inc.<sup>63</sup>

40 Facebook Ireland Ltd. is an establishment of Facebook Inc. pursuant to Recital 19 Data Protection Directive.<sup>64</sup> Article 4 I a) Data Protection Directive then provides that each Member State shall apply the national provisions to the processing of personal data where "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".

41 According to the submission of Facebook Ireland Ltd. in the following court proceedings, Facebook Inc. processes data on behalf of its Irish subsidiary. Thus, Facebook Inc. informed the ULD that for matters regarding European users, all enquiries must be directed to Facebook Ireland Ltd.<sup>65</sup>

42 In addition, the existing German Facebook subsidiary (Facebook Germany GmbH) is expressly not involved in the processing of any personal information. It merely handles marketing and acquisition for the local market only, and thus cannot be considered an establishment of the controller of personal data.<sup>66</sup>

43 Finally, Facebook Ireland Ltd. fully complies with Irish data protection laws, which are themselves compliant with European data protection law.<sup>67</sup> In Facebook's view, this was confirmed by the Irish Data Protection Authority as part of its audit reports dated December 2011 and September 2012.<sup>68</sup> As Irish law applies, § 13 VI of the TMG is not applicable to Facebook. In addition, this section of the TMG would infringe higher-ranking European law.

44 Even if § 13 VI TMG were applicable, a departure from its real name policy would not be reasonable for Facebook as it would put Facebook's "culture of true identity" at risk.<sup>69</sup> Facebook stressed that it intends to replicate the social norms of the real world in an online environment by "emphasizing the human qualities of conversation and sharing".<sup>70</sup> According to Facebook, users want and expect their relations on Facebook to be authentic.<sup>71</sup> The pseudonymous use of Facebook would destabilize the integrity of Facebook and undermine the trust that is necessary

to interact on Facebook.<sup>72</sup> The requirement of true identity is furthermore intrinsically tied to the security of users on the platform and an essential part of the security measures it implements.<sup>73</sup> Without these measures, safety, security and the integrity of the platform would be compromised significantly.<sup>74</sup> This reasoning was supported by Facebook's allegation that the vast majority of disabled Facebook accounts could be linked to spamming, distributing malware, phishing, trolling, cyber mobbing, dissemination of hate speech, distribution of child abuse materials and gaming cheats.<sup>75</sup>

## II. The court proceedings

- 45 Facebook lodged an objection to the order with the responsible administrative authority. It also filed an appeal to the Verwaltungsgericht (administrative court) and succeeded in restoring the suspensory effect of the objection, hence making the order not immediately enforceable.<sup>76</sup> The decision was subsequently affirmed by the appeal court.<sup>77</sup> Accordingly, Facebook does not have to unlock the accounts of those users in Schleswig-Holstein who used Facebook under a pseudonym and had been blocked.
- 46 Although the court held that the mandatory real name policy violates § 13 VI TMG, this was of no relevance as neither the TMG nor German data protection laws were applicable. Irish data protection law, which instead applies, does not foresee an explicit right to pseudonymous or anonymous use of telemedia services.
- 47 Unfortunately, the courts did not really question the facts presented by Facebook, because proceedings for preliminary measures require only a summary examination of the merits of the claim. Thus, there was no need to examine how and by whom data processing in the case in question takes place. For this reason, the decisions of the courts will only be discussed briefly.

### 1. No choice of law by Section 16.1 of the Statement of Rights and Responsibilities of Facebook

- 48 First of all, section 16.1 of Facebook's "Statement of Rights and Responsibilities" does not stipulate an application of material German data protection law.<sup>78</sup> In general, parties to a contract can agree that the contract shall be governed by the law chosen by them (Art. 3 I Rome I Regulation<sup>79</sup>). However, § 1 V BDSG, which prescribes the application of German law, constitutes an overriding mandatory provision in the sense of Article 9 Rome I Regulation. Hence, the application of German data protection law is not at the disposal of the parties, but has to be deter-

mined solely on the basis of § 1 V BDSG.<sup>80</sup> § 1 V BDSG, which transposes Article 4 I Data Protection Directive into German law, sets forth that the BDSG, and thus German data protection, shall not apply in so far as a controller located in another EU/EEA Member State collects, processes or uses personal data inside the country, except where such collection, processing or use is carried out by an establishment inside the country. The BDSG shall, however, apply in so far as a controller not located in an EU/EEA Member State collects, processes or uses personal data inside the country.

## 2. Data controller and establishment

- 49 The court based its findings primarily on the fact that the processing of personal data was not carried out at the German subsidiary "Facebook Germany GmbH". The court was satisfied that the processing of personal data actually took place in Ireland by Facebook Ireland Ltd. in the context of its own activities.<sup>81</sup> Thus, it concluded that Irish data protection law is exclusively applicable in accordance with Article 4 I a) Data Protection Directive.<sup>82</sup> As opposed to Facebook Germany GmbH, Facebook Ireland Ltd. was considered to be an establishment of Facebook Inc. in the sense of Article 4 Data Protection Directive. It was of no relevance that the traffic data of Facebook is processed in the US, and most content data are collected in Germany and stored and processed in Germany by the service provider Akamai. The court argued that whenever a data controller has an establishment in the EU/EEA Member State, it is of no relevance for the determination of applicable law whether he uses equipment in a third Member State.

## III. The question of "who is doing what?"

- 50 As mentioned previously, neither the Verwaltungsgericht (VG) Schleswig nor the appeal court, Oberverwaltungsgericht (OVG) Schleswig, asked Facebook to provide evidence on where the data is actually processed and by whom, because this was not necessary in preliminary proceedings where only a summary examination of the submissions of the parties is conducted. The courts merely accepted Facebook's submission as indicating data processing in Ireland. At this stage of the proceedings, there was little more to expect by the judges.
- 51 There are strong indications that Facebook Ireland Ltd. only plays a minor role in the processing of personal data, if it plays any at all. For example, Facebook Ireland Ltd. repeatedly argued that "certain things are not possible because the management of Facebook Inc. would never agree to them".<sup>83</sup> This

raises the question whether Facebook Ireland Ltd. has any control over the www.facebook.com platform that is technically hosted in the US. If Facebook Ireland Ltd. is not the actual data controller, but just a branch that has been set up to benefit from advantageous Irish tax law and fulfil some alibi tasks, then Article 4 I a) Data Protection Directive does not lead to an application of Irish data protection law. If the ULD pursues the matter further, then Facebook Ireland Ltd. will need to prove that it processes the personal data in question itself. It is not established that the court in the main proceedings will be satisfied as easily as the administrative court in the proceedings for interim measures. Thus, it is not unlikely that in the main proceedings, a court will come to a different conclusion. Also, another conclusion must not necessarily be contrary to the findings of the Irish Data Protection Commissioner in his Audit Reports of Facebook Ireland Ltd. He did not legally assess whether Facebook Ireland Ltd. is a data controller pursuant to Article 2 d) Data Protection Directive. Although there are indications as to Facebook Ireland Ltd.'s role ("It is the only office, and legal entity, within the Facebook group with control over non-North American user data." and "FB-I's staff (around 326 Full Time Employees and 75 contractors) are responsible for the development and maintenance of the Facebook platform, the protection of Facebook users, the corporate administration of many of Facebook's non-North American activities and the sale of advertising to customers."),<sup>84</sup> the Data Protection Commissioner refrained from analysing the control element of Facebook Ireland Ltd. In this context, the function of Facebook's offices in other Member States also need to be assessed. In the Audit Report of Facebook Ireland Ltd., it has been stated that

*[t]hese offices have no role in the development or maintenance of the platform or the control of user data. Their functions are limited to the sale of advertising, local PR and, in limited cases, addressing queries from local app developers. In the context of carrying out these duties, these offices may process a limited amount of user data relating to the pages of advertisers and prospective advertisers pursuant to processing agreements entered into with FB [Ireland].<sup>85</sup>*

- 52 Here, the scope of "limited amount of user data" needs to be assessed.
- 53 Beside Facebook's submissions, there is not yet enough evidence on where data is processed and by whom. The ULD now even succeeded in using some findings in the Audit Reports of the Office of the Irish Data Protection Commissioner to support its position.<sup>86</sup> In its Audit Report of 2012, the Irish Commissioner expressed concerns that "products and features developed by engineers predominantly based in California ... will not be capable of fully understanding and complying with Irish and EU data protection requirements".<sup>87</sup> Thus, Facebook Ireland Ltd. had to commit itself in the 2012 Re-Audit to imple-

ment measures "for ensuring that the introduction of new products or uses of user data take full account of Irish data protection law"<sup>88</sup>. Hence, the Facebook Ireland Ltd. data protection compliance team now examines compliance with Irish law.<sup>89</sup> This, however, rather indicates that the policies are determined by Facebook Inc., with Facebook Ireland Ltd. only having the possibility to intervene. Consequently, it is not Facebook Ireland Ltd. that determines the means and purposes of data processing on its own.<sup>90</sup>

- 54 A similar practice was identified by the Irish Data Protection Commissioner in relation to the implementation of new features, such as the "find your friends nearby" feature, for example: Facebook Inc. determines practices in the US while only foreseeing "input" from Facebook Ireland Ltd.<sup>91</sup> One may thus question whether Facebook Ireland Ltd. may instruct Facebook Inc. in any way in relation to the processing of personal data. It seems to have no competence to oversee the data processing by its parent company.
- 55 In addition, several incidents in the past show that the role of Facebook Ireland Ltd. with regard to data processing is less than clear. For example, in relation to Facebook's face recognition feature, Facebook did not succeed in proving that Facebook Ireland Ltd. guided and directed Facebook Inc. regarding the processing of personal data of European users.<sup>92</sup> In this case, it was not the ULD but the Data Protection Commissioner of Hamburg who issued an order against Facebook claiming that the feature violates German data protection law.<sup>93</sup> There was not sufficient evidence to prove that Facebook Ireland Ltd. was the actual data processor or directs the data processing of Facebook's face recognition feature.<sup>94</sup> The Hamburg Data Protection Commissioner's reasoning was very similar to that of the ULD, holding that the mere establishment of Facebook in Ireland does not automatically lead to the application of Irish data protection law; only where an establishment holds actual control for the data processing may it fall within the Data Protection Directive's definition of establishment. In relation to the face recognition feature, all decisions regarding the collecting, processing and use of data that were of relevance were taken by Facebook Inc. outside of the European Union.<sup>95</sup> Unfortunately, this case did not reach the trial stage as Facebook disabled the face recognition feature for European users.<sup>96</sup> Thus, until now, there is no precedent that has thoroughly examined Facebook's data processing.
- 56 Of particular interest in that context are furthermore the experiences of the Ministry of Justice of the German State of Baden-Württemberg with Facebook Ireland Ltd. when it comes to judicial cooperation requests in criminal matters and the access of German law enforcement agencies to data held by Facebook. To the knowledge of the Ministry of Justice, all of



Facebook's data are stored solely in the USA, and neither the establishment of Facebook in Germany nor Facebook Ireland Ltd. has direct access to the data.<sup>97</sup> This is a strong indication that Facebook Ireland Ltd. is not even involved in the data processing. Furthermore, Facebook Germany GmbH stated in criminal proceedings before a German criminal court that all servers that contain personal data of Facebook users are possessed and operated by Facebook Inc. in the US.<sup>98</sup> Facebook Germany could not tell whether the data requested in these proceedings were stored on servers of Facebook Inc. as only competent staff of Facebook Inc. could do so.<sup>99</sup> Again, there was no mention of the role of Facebook Ireland Ltd. in the actual processing. This shows, however, that Facebook is actually skating on very thin ice in the real name policy case when they argue that the data controller of personal data of European users is Facebook Ireland Ltd. and not Facebook Inc. In light of the above-mentioned incidents, it seems rather unlikely that they would succeed in proving that Facebook Ireland Ltd. is controlling the platform.

### C. The case in a wider context: The benefits of anonymity v. the drawbacks of anonymity

- 57 Irrespective of the applicable law, one should not lose sight of the initial question of the *ULD v. Facebook* case, namely whether real name policies may efficiently ban anti-normative and anti-social behaviour.
- 58 Facebook's main argument for enforcing its real name policy is that it is a fix for trolling and other unwanted behaviour. Clearly, it is not just teenage girls who change their last name to Bieber to imply marriage to the pop star Justin Bieber who are choosing to use a made-up name on a social network. But whether people really "behave a lot better when they have their real names down"<sup>100</sup> has not been proven by Facebook. Whether anonymity or pseudonymity mitigates social norms and establishes conditions to neglect principles of mutual respect in such a dimension as to outweigh the benefits of pseudonymous use is questionable.
- 59 Anonymous speech existed well before the advent of the Internet. But as the Internet magnifies speech to an exceptional level,<sup>101</sup> a new dimension is added to anonymous speech which also includes pseudonymous speech. Postings are instantaneously accessible worldwide, and thus are communicated to an undefined audience largely without any restrictions. A user may have good reasons to preserve his anonymity, especially where strong opinions are concerned. Anonymity may encourage people to express opinions, reveal something personal about themselves or engage in online activities that they otherwise would not express if the opinion or activity could be attributed to them.<sup>102</sup> Such cases include abuse victims who may wish to remain anonymous, or anyone else who fears unpleasant consequences when identified.<sup>103</sup> This could most recently be witnessed during the Arab spring, where many political dissidents posted information about the regimes' repercussions against civilians. It was the perceived anonymity on the Internet that allowed them to disseminate material without fear of consequences. Research in the early days of the Internet also proved that membership in gay/lesbian newsgroups and the available opportunity to share one's experiences and emotions anonymously and freely led to an increased self-acceptance of these individuals.<sup>104</sup> Online anonymity may also help young people in their own personal development as they express themselves without any negative social consequences.<sup>105</sup> These speakers do not commit any wrong by posting their opinions or experiences but may fear becoming subject to backlashes.
- 60 While there are good reasons to remain anonymous and anonymity may encourage free speech, it may also discourage responsibility.<sup>106</sup> Online anonymity is not always used for a good purpose: users may abuse anonymity to engage in anti-normative or anti-social behaviour. Undeniably, anonymity constitutes a disinhibiting factor that affects what people are prepared to say in computer-mediated communication.<sup>107</sup>
- 61 Anonymity has traditionally been thought to be more likely to create negative outcomes.<sup>108</sup> Obviously, anonymous as well as pseudonymous speech poses challenges to the tort of defamation and other unwanted behaviour.<sup>109</sup> Hence, Facebook argues that by enforcing the real name policy, it is pursuing a mission of trust and security. Google CEO Eric Schmidt went even a step further and called online anonymity "dangerous".<sup>110</sup> This may refer to the fact that people may hide behind their perceived anonymity and defame third parties; but it also may refer to the fact that although an Internet service provider is not liable for all content, it may be equally responsible for the content to some extent.
- 62 The use of nicknames and fake names may put victims of cyber bullying and defamation in a difficult position: where there are no clues and evidence in relation to the true identity of the perpetrator, the victims need to obtain a disclosure order against the Internet service provider in order to obtain further information so that the perpetrator may be held accountable. Even then the disclosure of the identity of an anonymous poster is only possible to a certain extent, namely tracing back his IP address, which can be time- and cost-consuming.<sup>111</sup> A defamation victim will have to obtain an order against the Internet service provider for disclosure of the registration data provided by the alleged tortfeasor, in-

cluding his email address and the IP addresses of all computers used to access the Internet service using that particular registration data. In the following a further disclosure order against the Internet access provider is needed to obtain the account subscriber's details. An IP address alone is not sufficient to identify the actual tortfeasor. Even where the Internet access provider holding information about the subscriber of a specific IP address at a certain time discloses the identity information following a court order, the information may not be sufficient to identify the tortfeasor where a connection is shared by several users. Thus, instead of trying to uncover the identity of an author and then proceed in suing him directly, defamation victims may turn to bringing an action against the Internet service provider to block access to the defamatory post if it does not do so voluntarily.<sup>112</sup> In this regard, due to the ubiquitous nature of the Internet, they may also be faced with questions of jurisdictions and immunities afforded to online intermediaries, such as those stemming from the E-commerce Directive.<sup>113</sup> A real name policy, where each communication can be attributed to a real person, would immediately eliminate these problems for defamation victims. However, a real name policy can only work where the registration data has been verified. Even then, someone may get access to a third party's account, most likely where unsecure passwords are used.

- 63 There clearly is a conflict between protecting online anonymity/pseudonymity and the equally privacy-related question of accountability for anti-normative behaviour. As relates to a mandatory real name policy, one should take into consideration whether a real name policy can succeed in fixing anti-social and anti-normative behaviour. In this respect, there is even evidence from a country that experimented with mandatory real names on a large scale. In 2007, South Korea implemented a real name verification law. The law required participants of discussions on the Internet to pass a verification process in order to express their opinions on websites with over 100,000 viewers.<sup>114</sup> The goal of this law was to reduce undesirable and anti-normative postings by changing the level of anonymity in which linkability and traceability are enhanced.<sup>115</sup> Although some suggested that the law had some effects on user behaviour,<sup>116</sup> a study by the Korea Communications Commission found that the system had been ineffective in preventing people from posting abusive messages.<sup>117</sup> In fact, malicious comments decreased by only 0.9% in 2008.<sup>118</sup> The Korean case provides real-life evidence that fear of judgement will not significantly change online behaviour for the better.<sup>119</sup>
- 64 The effect on other anti-social or illegal behaviour also has not been clearly proven. Facebook Ireland Ltd. described that Facebook's User Operations Team takes substantial efforts to investigate potential fake and imposter accounts created by adults

to make contact with teenagers, created by teenagers to bully other teenagers and created by adults to harass others.<sup>120</sup> Unfortunately, Facebook has refrained from making publicly available any statistics of fake identities used for anti-normative or anti-social behaviour. Instead it emphasises the importance of real identities to protect children in the online space.<sup>121</sup> This argument is weak considering that Facebook does not allow children under the age of 14 to register. Obviously, grooming is a problem on the Internet, but a real name policy does not prevent grooming, nor is grooming a substantial problem for Facebook where users usually interact with "friends".

- 65 Facebook's long-standing policy of making people use their real name also did nothing to prevent people using the social network to insult others. A real name policy is also no fix to the phenomenon of cyber bullying. Cyber bullying continues regardless of whether real names are used or not. Research has shown that cyber bullying often occurs in the context of social relationships, which challenges the assumption that it is anonymous.<sup>122</sup> In the recent prominent case of Amanda Todd, who committed suicide after being bullied on Facebook, bullying occurred by classmates and acquaintances.<sup>123</sup> It seems that online communication is merely an additional channel for traditional bullying, though anonymity may have a disinhibiting effect on what is posted. Other than the slanderous words, bullying on Facebook is fixed. However, the roots for bullying lie in the real social environment.<sup>124</sup>
- 66 Thus, Google CEO Eric Schmidt's assumption that online anonymity is "dangerous" is not true as such. Similarly, the argument that Facebook pursues a mission of trust and security does not seem convincing. Anonymous speech has its pros and cons, but there is nothing to suggest that a real name policy is a fix to anti-normative or anti-social behaviour. It may limit such behaviour, but whether that extent outweighs the advantages of anonymous speech is questionable. Allowing the pseudonymous use would also not hinder Facebook from employing security measures such as access control and authentication mechanisms, which can still be used where pseudonyms are permitted.

## D. Conclusion

- 67 It is of particular interest how this case will proceed – not so much in terms of the real name policy but the applicable law to Facebook. The real name policy is what triggered the discussion of a much wider issue, namely whether Facebook can carry on showing little regard for the privacy of its users and ignore national privacy laws.

- 68 The question of who controls Facebook is substantial. Are national efforts to regulate futile against a globalised multinational cooperation? If each state asserts jurisdiction over the same website, then inevitably the rules for users around the world will vary depending on their residency. Facebook rules already vary to some extent, with a special set of rules applying only to users in Germany.<sup>125</sup> Germany has been deemed the fiercest critic of Facebook due to its deep commitment to privacy.<sup>126</sup>
- 69 Facebook can escape the application of strict German law only if Facebook Ireland Ltd. is the controller of personal data processing and no establishment of Facebook controls user data in Germany. The Facebook companies thus will have to disclose their internal organisational structure for the processing of personal data. As of now, Facebook's external presentation does not distinguish between Facebook Ireland Ltd. and Facebook Inc., so the companies and their activities are difficult to separate from each other.<sup>127</sup>
- 70 In a wider context and with regards to competent supervisory authority in such matters, the case could set a precedent and render the implementation of a one-stop-shop solution as favoured by European Commissioner for Justice Viviane Reding unnecessary. Reding has been supporting "one-stop shop" for the clarification of data protection questions – a unified EU policy and a clear point of contact for every company. The European Commission's draft for a new EU data protection regulation proposes that in situations where Internet companies have several offices in Europe, the supervisory authority for those companies should be handled by the Member State in which they have their European headquarters.<sup>128</sup> For Facebook, this would mean that the Irish government's Data Protection Commissioner would be responsible for the concerns of all EU citizens relating to the company's privacy policies because the headquarters are in Ireland. Such a centralisation of supervisory authority has been criticised by the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament under Rapporteur Jan Philipp Albrecht. Under his draft of a new data protection regulation, EU data subjects would still be able to address the authority in their place of residency and in their own language.<sup>129</sup> Each applicable data protection authority would be competent to supervise processing operations within its territory or affecting local data subjects. The local supervisory authority in the Member State would be competent but not solely responsible. There will be a lead supervisory authority at the place of the main establishment which acts as a single contact point for the controller or the processor and ensures coordination with all other data protection authorities involved.<sup>130</sup> The lead authority shall also consult the other authorities before adopting a measure.<sup>131</sup> Under the Albrecht Draft, there would also be a European Data Protection Board equipped with a veto power which may adopt a final decision. Under the Reding Draft, the European Commission would have had the final word in unresolved disputes.
- 71 The Reding Draft as well as the approach by the appeals court OVG Schleswig are clearly advantageous for companies that process personal data. They have a single point of contact for resolving issues. As a consequence, this could lead to business corporations establishing their European headquarters where data protection supervision is weak. As of now, Facebook has chosen Ireland as the place for its European headquarters due to advantageous tax laws, but it is not unlikely that corporations may seek lax data protection supervision in future. The same competition between countries could occur in relation to data protection as is known from the field of tax law.<sup>132</sup>
- 72 As concerns real name policies in general, providers of social networks clearly have identified the potential of big data and aim to monetize the accumulated data as business entities. Specifically, Facebook is considered so valuable because it is in fact a data machine that retains every mouse click and interaction of its users.<sup>133</sup> With Facebook's vast database of users' likes, relationship statuses, personal information, photos and shares, it can offer advertisers the possibility to target their ads to the right audience.<sup>134</sup> By the ubiquitous "like" button, Facebook is able to compile consumer profiles. In addition, the Facebook Connect service allows users to log into millions of websites using their Facebook user ID and password, and also reports back about their activity on those sites.<sup>135</sup> In the following, Facebook can sell advertising space to advertisers that allows them to precisely address the audience they covet.<sup>136</sup> This function is not disabled by users using pseudonyms, however. Their consumer behaviour and consumer profile can still be tracked; the only difference is that the data subject acts under a fake name.
- 73 Being forced to abandon the real name policy would not jeopardise the future of Facebook. However, it influences the value of Facebook. Facebook's shares lost almost half their value following revelations that as many as 8.7% of Facebook's 955 million user accounts may be fake and up to 5% of active accounts duplicates.<sup>137</sup> It may also put at risk further business models of Facebook. Facebook already serves as an identity provider by offering other websites use of its identity system rather than requiring users to create a new profile. One may also think that user information on Facebook is used to determine the creditworthiness of said user. This idea is not as far-fetched as one might think. In 2012, a German credit agency commissioned a research project to use Facebook to study a person's relationships in order to determine how that might affect their ability to pay their bills.<sup>138</sup> Following protest by German pol-

iticians such as the German Justice Minister at that time, Sabine Leutheusser-Schnarrenberger (“It cannot be that Facebook friends and preferences lead to one, for example, not being able to get a cell phone contract”<sup>139</sup>), the research project was withdrawn.<sup>140</sup> Such a use of Facebook data would be an entirely new dimension. Although the study has never been conducted, the idea of the project highlights the potential of Facebook’s big data.

74 Finally, the legal battle against Facebook’s real name policy highlights the struggle of service providers operating worldwide to adapt their service to the legal regimes governing the markets they have entered. The number of legal actions, and in particular the case of *ULD v. Facebook*, is set to continue, but for now we have to say good-bye to Max Mustermann.

- 1 Sobel, “*The Process that ‘John Doe’ Is Due: Addressing the Legal Challenge to Internet Anonymity*” [2000] 5 Virginia Journal of Law and Technology 3.
- 2 Google+’s common name policy as of June 2013: <<http://support.google.com/plus/answer/1228271?hl=en&uls=en>>; Facebook’s real name policy as of June 2013: <<http://www.facebook.com/help/292517374180078/>> (accessed 3 June 2013).
- 3 In the following, the author tries to distinguish between statements by Facebook Inc. and its subsidiaries; however, where the distinction is of no relevance or statements are issued on behalf of Facebook in general, the author refers to “Facebook” only.
- 4 See sec. 19.1 of Facebook’s Statement of Rights and Responsibilities at <<http://www.facebook.com/legal/terms>> (accessed 3 June 2013).
- 5 Ireland has a 12.5% corporate tax rate; the rate in the US is 35%. By making use of the so called “double Irish” global tax strategy, which involves Irish subsidiaries and subsidiaries in offshore locations, the corporation tax can be reduced further to about 2-3% corporation tax on all international revenue. Keena, “Ireland helps Facebook save billions” (14 May 2012), <<http://www.irishtimes.com/newspaper/finance/2012/0514/1224316065838.html>> (accessed 3 June 2013).
- 6 See the introductory paragraph (last updated: 8 June 2012), <[https://www.facebook.com/legal/terms?locale=en\\_EN](https://www.facebook.com/legal/terms?locale=en_EN)> (accessed 3 June 2013).
- 7 Ibid.
- 8 As a contractual choice-of-law clause, this clause does not affect tort actions, of course.
- 9 According to sec. 17 of the Statement, Facebook “strive[s] to create a global community with consistent standards for everyone, but [...] also strive[s] to respect local laws”. Hence, this section contains provisions that apply only to users and non-users that interact with Facebook outside the US. While subsection 1 relates to data transfer and processing in the US and subsection 2 to an exclusion of commercial activities by countries embargoed by the US, subsection 3 provides a hyperlink to specific terms that apply only to Germany.
- 10 Section 5 of the rules for users with German residency (last revised 20 April 2012), original wording: “5. Ziffer 16.1 wird ersetzt durch: Diese Erklärung unterliegt deutschem Recht”, <<https://www.facebook.com/terms/provisions/german/index.php>> (accessed 3 June 2013).
- 11 See Facebook Data Use Policy (last revised 11 December 2012), <[https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy)> (accessed 3 June 2013).
- 12 Max Mustermann is the German “Joe Doe”.
- 13 The so-called “Beliebers”, fans of pop star Justin Bieber, change their name to give the impression that they are married to their pop idol. Adrienne Jeffries, “Facebook’s fake-name fight grows as users skirt the rules” (17 September 2012), <<http://www.theverge.com/2012/9/17/3322436/facebook-fake-name-pseudonym-middle-name>> (accessed 3 June 2013).
- 14 <<http://www.facebook.com/help/292517374180078/>> (accessed 3 June 2013).
- 15 Ibid.
- 16 Ibid.
- 17 Sengupta, “*Lady Gaga Now, Even on Facebook*” (16 February 2012), <[http://www.nytimes.com/2012/02/17/technology/new-facebook-policy-on-made-up-names-lets-gaga-be-gaga.html?\\_r=3&](http://www.nytimes.com/2012/02/17/technology/new-facebook-policy-on-made-up-names-lets-gaga-be-gaga.html?_r=3&)> (accessed 3 June 2013).
- 18 Ibid. The verification procedure requires users to send an image of their passport or other form of ID to Facebook.
- 19 See di Fabio in: Maunz, Dürig, et al. (eds.), *Grundgesetz* (Kommentar, Beck München 69th ed. 2013), Art. 2 paras. 173 to 191; Foster and Sule, *German Legal System and Laws* (Oxford, 4th ed. 2010), pp. 241 et seq.
- 20 Author’s own translation.
- 21 Respectively § 4 I (from 2001 onwards § 4 VI) Teledienstdatenschutzgesetz (TDDSG) and § 13 I (from 2002 onwards § 18 VI) Mediendienststaatsvertrag (MDStV).
- 22 The Bundesdatenschutzgesetz.(BDSG) transposes the Data Protection Directive 95/46/EC into German law.
- 23 In comparison, § 3 VI BDSG defines “rendering anonymous” as meaning the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person or that such attribution would require a disproportionate amount of time, expense and effort.
- 24 Müller-Broich, *Telemediengesetz* (Nomos-Kommentar, Nomos Baden-Baden 2012), § 13 TMG.
- 25 Ibid.; Spindler & Nink in: Spindler & Schuster (eds.), *Recht der elektronischen Medien* (Kommentar, Beck München 2nd ed. 2011), § 13 TMG para. 10.; Deutscher Bundestag, “Drucksache 13/7385” (1997), p. 23, <<http://dipbt.bundestag.de/dip21/btd/13/073/1307385.pdf>> (accessed 3 June 2013).
- 26 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 (23 November 1995), pp. 31-50.
- 27 § 3a BDSG (Data reduction and data economy): Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.
- 28 Spindler & Nink (fn 25), § 13 para. 10.
- 29 BVerfGE 65, 1, 43; for an analysis of the population census decision and the “invention” of the basic right to informational self-determination, see Hornung & Schnabel, “Data protection in Germany I: the population census decision and the right to informational self-determination” [2009] 25 Computer Law & Security Review 84.
- 30 BVerfGE 65, 1, 43.
- 31 Spindler & Nink (fn 25), § 13 para. 10.
- 32 See OLG Hamburg, ZUM 2009, 417 at 420 – Long Island Ice Tea case.

- 33 OLG Düsseldorf, MMR 2006, 618 at 620.
- 34 Spindler & Nink (fn 25), § 13 para. 10.
- 35 The ULD Schleswig-Holstein (Independent State Centre for Privacy Protection of Schleswig-Holstein) is the office of the Data Protection Commissioner of the German state of Schleswig-Holstein. The ULD is the responsible authority to enforce data protection compliance at Facebook for data subjects in the German state of Schleswig-Holstein. Head of the ULD and Data Protection Commissioner of Schleswig-Holstein is Thilo Weichert, who has held the position since September 2004. The Commissioner is elected for a period of five years by the parliament of Schleswig-Holstein.
- 36 ULD, “ULD issues orders against Facebook because of mandatory real names” (17 December 2012), <<https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm>> (accessed 3 June 2013). See also Weichert, “Facebook, der Datenschutz und die öffentliche Sicherheit” in Möllers & van Ooyen (eds.), *Jahrbuch öffentliche Sicherheit 2012/2013* (Verlag für Polizeiwissenschaft Frankfurt 2012) p. 380.
- 37 The ULD – as the competent supervisory authority on data protection – is entitled to issue orders to ensure compliance with the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and other data protection provisions; see § 38 V BDSG. Such orders are not unfamiliar to Facebook. As recently as September 2012, the Hamburg Data Protection Commissioner issued an administrative order against Facebook in relation to the face recognition feature. Facebook was ordered to ask registered users for permission when generating and storing biometric profiles. In February 2013, the administrative proceedings were closed as Facebook was able to prove that its face recognition feature had been disabled in Europe. See press release of the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit of 7 February 2013, <<http://www.datenschutz-hamburg.de/news/detail/article/facebook-gesichtserkennung-verwaltungsverfahren-eingestellt.html>> (accessed 3 June 2013).
- 38 See Order of the ULD against Facebook Ireland Ltd. of 14.12.2012, <<https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-ltd.html>>.
- 39 See Order of the ULD against Facebook Ireland Ltd. of 14.12.2012, <<https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-ltd.html>>; Order of the ULD against Facebook Inc. of 14.12.2012, available at <https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-inc.html> (both accessed 3 June 2013).
- 40 In particular, the ULD applies § 1 V 2 BDSG: “This Act shall apply in so far as a controller not located in a European Union Member State or other state party to the Agreement on the European Economic Area collects, processes or uses personal data inside the country”. The section transposes Art. 4 I c) Data Protection Directive into national law.
- 41 See only Order of the ULD against Facebook Ireland Ltd. of 14.12.2012, <<https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-ltd.html>>.
- 42 See also Data Protection Commissioner, “Facebook Ireland Ltd - Report of Audit, 21 December 2011” (2011), p. 26, <<http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf>> (accessed 3 June 2013).
- 43 In this context, the ULD cited an example from the Opinion on applicable law by the Art. 29 Data Protection Working Party, where a social network had its headquarters in a third country and an establishment within an EU Member State. The establishment defined and implemented the policies relating to the processing of personal data of EU residents. The social network actively targeted residents of all EU Member States, which formed a significant portion of its customers and revenues, and installed cookies on EU users” computers (Article 29 Data Protection Working Party, “Opinion 8/2010 on applicable law, 0836-02/10/EN, WP 179” (2010), p. 27, <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf)> (accessed 3 June 2013)). According to the Art. 29 Data Protection WP, the applicable law will be, as set forth in Art. 4 I a), the data protection law of the place of establishment of the company within the EU. The ULD distinguished the situation of Facebook Inc. and Facebook Ireland Ltd. from the one in the example as there apparently was no evidence that Facebook Ireland Ltd. determines the business policy of Facebook in Europe, and in this context also determines the purposes for which the personal data of European users are processed (e.g. advertising, customised design of the service).
- 44 See also Appeal of the ULD against the decision of the VG Schleswig of 14 February 2013 relating to Facebook Inc., <<https://www.datenschutzzentrum.de/facebook/20130312-beschwerdebegrueundung-facebook-inc.html>> (accessed 3 June 2013).
- 45 *Ibid.*, p. 12.
- 46 *Ibid.*, p. 14.
- 47 Facebook has not yet provided the relevant agreements between Facebook Inc. and Facebook Ireland Ltd.
- 48 Appeal of the ULD against the decision of the VG Schleswig of 14 February 2013 relating to Facebook Inc. (fn 43).
- 49 ULD, “Anordnung der sofortigen Vollziehbarkeit von Untersagungsverfügungen im Hinblick auf den Klarnamenzwang bei Facebook” (2013), <<https://www.datenschutzzentrum.de/facebook/20130204-facebook-klarnamen.html>> (accessed 3 June 2013), which refers to ULD, “Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook” (2011), pp. 16 et. seq., <<https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf>> (accessed 3 June 2013).
- 50 According to § 3 VII BDSG, which transposes Art. 2 d) Data Protection Directive into German law, the responsible entity, i.e. the controller, “is any person or body which collects, processes or uses personal data on his, her or its or behalf, or which commissions others to do the same”.
- 51 ULD (fn 48), para. 3.
- 52 *Ibid.*
- 53 See Data Protection Commissioner (fn 41), p. 25.
- 54 See Order of the ULD against Facebook Ireland Ltd of 14.12.2012 (fn 39), para. B. a). Although the wording of the German transposition of Art. 2 d) Data Protection Directive does not explicitly mention the case of joint determination of purposes and means of data processing, the German provision has to be interpreted as also encompassing joint control. The ULD refers in this context to Article 29 Data Protection WP, “Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, 00264/10/EN, WP 169” (2010), p. 23 <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)> (accessed 3 June 2013).
- 55 It seems that this wording is taken from *ibid.*, p. 19.
- 56 *Ibid.*
- 57 Cf. § 2 No. 1 TMG, which transposes Art. 2 b) E-Commerce Directive into German law.
- 58 A large part of the ULD’s order deals with the proportionality of the ordered measures, i.e. whether the registration under a pseudonym, the unlocking of blocked pseudonymous accounts and the information of users about the possibility of pseudonymous use of Facebook are suitable and necessary to protect the fundamental rights of Facebook users, and whether they are reasonable. First of all, these measures pursue a legitimate aim in protecting the right to informational self-determination (Art. 2 I in connection with Art. 1 I of the Basic Law of Germany) of individuals who wish to use Facebook. It also protects the user’s constitutionally guaranteed freedom of expression, enshrined in Art. 5 of the Basic Law: freedom of expression is affected when users must

fear sanctions for alleged trolling. Also, the fact that only those who registered under their real name may speak at all was criticised for interfering with the right to informational self-determination.

- 59 See Order of the ULD against Facebook Ireland Ltd of 14.12.2012 (fn 39), para. B. e) (2).
- 60 Ibid.
- 61 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), Official Journal L 178 , 17.07.2000, pp.1 -16.
- 62 Order of the ULD against Facebook Ireland Ltd. of 14.12.2012 (fn 39), para. B. e) (4).
- 63 Hence, Facebook asked the ULD to issue all requests regarding the real name policy to Facebook Ireland Ltd. See Order of the ULD against Facebook Inc. of 14.12.2012, <<https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-inc.html>> (accessed 3 June 2013).
- 64 An establishment in that sense requires "the effective and real exercise of activity through stable arrangements".
- 65 Order of the ULD against Facebook Inc. of 14.12.2012 (fn 62), para. B. a).
- 66 A detailed analysis of Facebook's position can be found in ULD (fn 48), para. 3.
- 67 Ibid.
- 68 The Irish Data Protection Commissioner published a report on its one-year-long audit procedure in December 2011 and a "review of the report" in September 2012.
- 69 See Order of the ULD against Facebook Ireland Ltd of 14.12.2012 (fn 39), para. B. e) (2), and Data Protection Commissioner (fn 41), p. 136.
- 70 Ibid.
- 71 See Order of the ULD against Facebook Ireland Ltd of 14.12.2012 (fn 39), para. B. e) (2).
- 72 Ibid.
- 73 Ibid.
- 74 Ibid.
- 75 Ibid, para. B. e) (3).
- 76 VG Schleswig, decision of 14 February 2013 – file no. 8 B 60/12 (ULD v. Facebook Ireland Ltd), <<https://www.datenschutzzentrum.de/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf>>; and 8 B 61/12 (ULD v. Facebook Inc.), <<https://www.datenschutzzentrum.de/facebook/Facebook-Inc-vs-ULD-Beschluss.pdf>> (both accessed 3 June 2013).
- 77 OVG Schleswig-Holstein, decision of 22 April 2013 – file no 4 MB 10/13 (ULD v. Facebook Ireland Ltd.), <<https://www.datenschutzzentrum.de/facebook/20130422-ovg-beschluss-facebook.pdf>>; and 4 MB 11/13 (ULD v. Facebook Inc.), <<https://www.datenschutzzentrum.de/facebook/20130422-ovg-beschluss-facebook-inc.pdf>> (both accessed 3 June 2013).
- 78 Ibid.
- 79 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I Regulation).
- 80 See also Carlo Piltz, "Rechtswahlfreiheit im Datenschutzrecht, 'Diese Erklärung unterliegt deutschem Recht'", *Kommunikation und Recht* 2012, 645. However, there are strong arguments in favour of the choice of law also in relation to respective provisions of the BDSG and TMG as they do not only apply between public authorities and private parties but also between private parties as such; see LG Berlin, Decision of 06.03.2012 – case no. 16 O 551/10 (Facebook friends finder), *Kommunikation und Recht* 2012, 300, and Polenz, "Die Datenverarbeitung durch und via Facebook auf dem Prüfstand", *Verbraucher und Recht* 2012, 209, who additionally argues that even where there is a deriving choice of law, national law must be applicable for consumer contracts.
- 81 Cf. only VG Schleswig, decision of 14 February 2013 – file no. 8 B 60/12 (ULD v. Facebook Ireland Ltd) (fn 75).
- 82 Ibid.
- 83 Europe-v-Facebook.org, "Response to 'Audit' by the Irish Office for the Data Protection Commissioner on 'Facebook Ireland Ltd'". (2012), p. 17, <<http://www.europe-v-facebook.org/report.pdf>> (accessed 3 June 2013).
- 84 Data Protection Commissioner, "Facebook Ireland Ltd. - Report of Audit 21 December 2011, Appendices" (2011), p. 213, <<http://www.dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf>> (accessed 3 June 2013).
- 85 Ibid, p. 215.
- 86 Although the Irish Commissioner was satisfied that he has jurisdiction over the personal data processing activities of Facebook Ireland Ltd., he emphasised in his initial audit report that this position shall not be interpreted as asserting sole jurisdiction over the activities of Facebook in the EU; see Data Protection Commissioner (fn 41), p. 21.
- 87 Data Protection Commissioner, "Facebook Ireland Ltd. - Report of Re-Audit 21 September 2012" (2012), p. 53, <[http://dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf)> (accessed 3 June 2013).
- 88 Ibid.
- 89 Ibid, p. 54.
- 90 ULD (fn 48).
- 91 Data Protection Commissioner (fn 82), p. 54 et seq.
- 92 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, "Rechtliche Bewertung der Gesichtserkennung und Zuständigkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit" (2012), p. 4, <[http://www.datenschutz-hamburg.de/fileadmin/user\\_upload/documents/Gutachten\\_Facebook-Gesichtserkennung.pdf](http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Gutachten_Facebook-Gesichtserkennung.pdf)> (accessed 3 June 2013).
- 93 The Hamburg Data Protection Commissioner also held that Facebook Ireland Ltd. is not an establishment of Facebook Inc. in the sense of Art. 4 I a) Data Protection Directive. Order of the Hamburgischer Beauftragter für den Datenschutz und die Informationsfreiheit against Facebook of 21 September 2012 (Facebook's face recognition), p. 17, <[http://www.datenschutz-hamburg.de/uploads/media/Anordnung\\_gegen\\_Facebook\\_2012-09-21.pdf](http://www.datenschutz-hamburg.de/uploads/media/Anordnung_gegen_Facebook_2012-09-21.pdf)> (accessed 3 June 2013).
- 94 Ibid.
- 95 Ibid.
- 96 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Facebook Gesichtserkennung – Verwaltungsverfahren eingestellt (2013), <[http://www.datenschutz-hamburg.de/fileadmin/user\\_upload/documents/Presseerklaerung\\_2013-02-07-Facebook-Gesichtserkennung.pdf](http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Presseerklaerung_2013-02-07-Facebook-Gesichtserkennung.pdf)> (accessed 3 June 2013).
- 97 See Appeal of the ULD against the decision of the VG Schleswig of 14 February 2013 relating to Facebook Inc., <<https://www.datenschutzzentrum.de/facebook/20130312-beschwerdebegrueendung-facebook-inc.html>> (accessed 3 June 2013).
- 98 AG Reutlingen, order of 31 October 2011 – case no. Js 18155/10 jug, *Kommunikation und Recht* 2012, 303 et seq.
- 99 Ibid.
- 100 Former Facebook Marketing Director, Randi Zuckerberg, argued that she thinks "anonymity on the Internet has to go away....People behave a lot better when they have their real names down. ... I think people hide behind anonymity and they feel like they can say whatever they want behind closed doors". See Bosker, "Facebook's Randi Zuckerberg: Anonymity Online 'Has To Go Away'" (27 July 2011), <<http://www.huffing>

- tonpost.com/2011/07/27/randi-zuckerberg-anonymity-online\_n\_910892.html> (accessed 3 June 2013).
- 101 Murray, *Information Technology Law: The Law and Society* (1st ed. Oxford University Press 2010), p. 105.
- 102 Cassidy, Jackson & Brown, “Sticks and Stones Can Break My Bones, But How Can Pixels Hurt Me?: Students’ Experiences with Cyber-Bullying”, [2009] 30 *School Psychology International* 383; Maureen Daly, “Is there an entitlement to anonymity? A European and international analysis”, [2013] 35 *European Intellectual Property Review* 198, 198.
- 103 For further examples, see Vamialis, “Online defamation: confronting anonymity”, [2013] 21 *International Journal of Law and Information Technology* 31, 61.
- 104 See Christopherson, “The positive and negative implications of anonymity in Internet social interactions: On the Internet, Nobody Knows You’re a Dog”, [2007] 23 *Computers in Human Behavior* 3038, 3042 with further references.
- 105 Ibid.
- 106 Joint Committee on the Draft Defamation Bill, Draft Defamation Bill 2010-12, HL 203, HC 930-I, para. 102.
- 107 Cf. Eady in: Smith v. ADVFN Ltd [2008] EWHC 1797 (QB), para. 15. See also Chi En Kwan & Skoric, “Facebook bullying: An extension of battles in schools”, [2013] 29 *Computers in Human Behavior* 16, 18 et seq.
- 108 Christopherson (fn 103), 3050.
- 109 Vamialis (fn 102), 31.
- 110 See video of Techonomy conference at <http://techonomy.typepad.com/blog/2010/08/google-privacy-and-the-new-explosion-of-data.html>. The same policy was introduced by Google in relation to Google+ (accessed 3 June 2013).
- 111 In relation to English law, cf. for example Vamialis (fn 102), 43 et seq.
- 112 This problem has also been addressed by the Joint Committee on the Draft Defamation Bill, Draft Defamation Bill 2010-12, HL 203, HC 930-I, para. 100.
- 113 Cf. Arts. 12 to 15 E-Commerce Directive .
- 114 Cho, “Real Name Verification Law on the Internet - A Poison or Cure for Piracy?” (2011), p. 3, <http://weis2011.econinfosec.org/papers/Real%20Name%20Verification%20Law%20on%20the%20Internet%20-%20A%20Poison%20or%20Cu.pdf> (accessed 3 June 2013).
- 115 Ibid, p.5.
- 116 Ibid, pp. 9 et seq.
- 117 Chosun Media, “Real-Name Online Registration to Be Scrapped” (30 December 2011), <http://english.chosun.com/site/data/html\_dir/2011/12/30/2011123001526.html> (accessed 3 June 2013).
- 118 Ibid.
- 119 Ferenstein, “Surprisingly Good Evidence That Real Name Policies Fail To Improve Comments” (29 July 2012), <http://techcrunch.com/2012/07/29/surprisingly-good-evidence-that-real-name-policies-fail-to-improve-comments/> (accessed 3 June 2013).
- 120 Data Protection Commissioner (fn 41), p. 137.
- 121 Ibid.
- 122 Mishna and others, “Risk factors for involvement in cyber bullying: victims, bullies and bully-victims”, [2012] 34 *Children and Youth Services Review* 63, 64 with further references.
- 123 Mungin, “Bullied Canadian teen leaves behind chilling YouTube video” (13 October 2012), <http://edition.cnn.com/2012/10/12/world/americas/canada-teen-bullying> (accessed 3 June 2013).
- 124 Chi En Kwan & Skoric (fn 106), 24.
- 125 <https://www.facebook.com/terms/provisions/german/index.php> (accessed 3 June 2013).
- 126 Chander, “Facebookistan, Introduction to the North Carolina Law Review Symposium, Social Networks and the Law”, [2012] 90 *North Carolina Law Review* 1807, 1822.
- 127 For example, see Facebook key facts, <http://newsroom.fb.com/key-facts> (accessed 3 June 2013).
- 128 European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final” (3 February 2012), p. 12, <http://ec.europa.eu/justice/data-protection/document/review2012/com\_2012\_11\_en.pdf> (accessed 3 June 2013). Art. 51 of the proposed Regulation sets out the competences of the supervisory authorities. The general rule, based on Art. 28 VI of Directive 95/46/EC (competency on the territory of its own Member State), will be complemented by the new competence as lead authority in case a controller or processor is established in several Member States.
- 129 European Parliament - Committee on Civil Liberties Justice and Home Affairs, “Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)” (2012), pp. 162 et seq., <http://www.europarl.europa.eu/meetdocs/2009\_2014/documents/libe/pr/922/922387/922387en.pdf> (accessed 3 June 2013).
- 130 Ibid, p. 213.
- 131 Ibid.
- 132 For example, Luxembourg has attracted companies such as eBay and Amazon, which sell their products and services from Luxembourg with lower taxes.
- 133 Sengupta & Rusli, “Personal Data’s Value? Facebook Is Set to Find Out” (31 January 2012), <http://www.nytimes.com/2012/02/01/technology/riding-personal-data-facebook-is-going-public.html?pagewanted=all&r=0> (accessed 3 June 2013).
- 134 See Facebook’s data usage policy, “IV. How advertising and Sponsored Stories work” (last revised 11 December 2012), <https://www.facebook.com/full\_data\_use\_policy> (accessed 3 June 2013).
- 135 Ibid.
- 136 Ibid.
- 137 Rushe, “Facebook share price slumps below \$20 amid fake account flap” (3 August 2012), <http://www.guardian.co.uk/technology/2012/aug/02/facebook-share-price-slumps-20-dollars> (accessed 3 June 2013).
- 138 Medick & Weiland, “German Credit Agency Plans to Analyze Individual Facebook Pages” (07 June 2012), <http://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html> (accessed 3 June 2013).
- 139 Ibid.
- 140 ore/dpa, “Facebook: Institut sagt Schufa-Schnüffelforschung ab” (8 June 2012), <http://www.spiegel.de/netzwelt/netzpolitik/facebook-institut-sagt-schufa-schnueffel-forschung-ab-a-837762.html> (accessed 3 June 2013).