Face Recognition Privacy in Social Networks under German Law

Yana Welinder examines the Hamburg Data Protection Agency's forthcoming action to show how the German Federal Data Protection Act regulates automatic face recognition in social networks.

One November day, a college student—let's call him "Andy"—was walking to his locker when he was approached by a researcher. The researcher asked Andy to participate in a study to try to find his Facebook profile based on three photos of his face. Andy was intrigued—not least because he had already deleted his Facebook profile picture from his account. As a senior and soon to enter the job market, he was concerned about the countless embarrassing status updates and photos he had posted during his college years. After taking three photos of Andy, the researcher asked him to fill out an online questionnaire. Clicking through to the last page of the questionnaire, Andy was stunned to find his entire Facebook profile on the screen, with his name, in a big black font, next to Facebook's blue default avatar.

This remarkable study was conducted by researchers at Carnegie Mellon University "to show that it is possible to start from an anonymous face in the street, and end up with very sensitive information about that person."[1] The study exemplified how the vast amount of personal information in social networks can be misused to essentially place a nametag on each individual as she walks around in public. While Facebook introduced face recognition technology on its website around the same time as this study was conducted, the researchers did not use Facebook's technology.[2] Instead, they used publicly available face recognition technology and photos that could be viewed on Facebook without logging in.[3] When combining these two resources, they were able to identify roughly one of three participants in only a few seconds.[4] They could even identify "Andy" despite the fact that he had no profile picture because he was "tagged" in his friends' photos.[5]

The recent developments in face recognition technology are what the 1983 German Constitutional Court would describe as the "pressure of the modern information use" upon an individual's right of self-determination—more specifically, an individual's right to decide whether to remain anonymous in public.[6] The constitutional "right of informational self-determination" is at the heart of the German Federal Data Protection Act, which the Hamburg Data Protection Agency recently alleged Facebook to be violating.[7] This article first discusses Facebook's face recognition technology to illustrate how such technology can connect an otherwise anonymous face to personal information in social networks. It then focuses on the Hamburg Data Protection Agency's forthcoming action to show how the German Federal Data Protection Act regulates automatic face recognition in social networks. Finally, this article analyses the relevant choice of law and jurisdiction provisions to explain why the Hamburg Data Protection Agency can threaten legal action against Facebook for the violation of German law.

The constitutional "right of informational self-determination" is at the heart of the German Federal Data Protection Act, which the Hamburg Data Protection Agency

I. Face Recognition Technology and Facebook

A. Brief Overview of the Technology

Face recognition technology aims to combine the superior human perception skills with the immense memory capacity of computers. Humans recognize other individuals visually based upon their appearances—focusing on facial features—and by using other senses, such as smell, hearing, and sometimes touch.[8] They also greatly rely on "context," such as an individual's clothing style, the surrounding people, the environment, and geographic location.[9] But while recognition is a natural human skill, the human brain can only memorize a limited number of faces.[10] Computers, on the other hand, can process and remember a vast amount of facial features to recognize many more people.[11] Qualitatively, however, computers do not compare to human recognition because they are still unable to combine visual recognition with other human senses and lack "contextual knowledge."[12]

---

1 Alessandro Acquisti, Ralph Gross, and Fred Stutzman, Faces of Facebook: *Privacy in the Age of Augmented Reality,* Heinz College, Carnegie Mellon University, available at http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/ (last visited Apr. 25, 2012), video presentation of research from the 2011 Black Hat Briefings Technical Information Security Conference available at http://www.youtube.com/watch?v=fZQ7Th9L5ss (last visited Apr. 25, 2012). While this study was able to find a Facebook profile for an individual who did not have a profile picture, the other facts in the story about "Andy," as well as his name, are purely fictional.

2 *Id.*

3 *Id.*

4 *Id.*.

5 *Id.*

6 Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination,* 37 Am.J.Comp.L. 675, 687 (1989).

7 Id. at 675; Press Release, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Facebook's Biometric Database Continues to be Unlawful (Nov. 10, 2011) ("Hamburg DPA November 10 Press Release"), available at http://www.datenschutz-hamburg.de/uploads/media/PressRelease-2011-11-10-Facebook_BiometricDatebase.pdf (last visited Nov. 14, 2011).

8 Wenyi Zhao & Rama Chellappa, Face Processing: Advanced Modeling and Methods 8-9 (Elsevier Academic Press 2006).

9 *Id.*

10 *Id.*

11 *Id.*

12 *Id.*

Generally,[13] automatic face recognition starts with measuring facial features of individuals that have already been identified in photos.[14] These measurements—which make up their unique "biometric data"—are then compiled into a "biometric database."[15] Face recognition technology is then applied to a new photo to find a face and detect its features.[16] The face is then "normalized," which entails transforming its scale, position, and light, and sometimes converting it into a gray-scale image.[17] The technology then measures the facial features in the photo and compares the resulting biometric data to the previously compiled database to identify the newly detected face.[18]

Facebook's photo collection contained around 100 billion photos by mid-2011 and was estimated to have increased by 6 billion photos each month.

The accuracy of automatic face recognition depends upon factors such as the exact methodology of the process described above, the number of available photos when creating the database, the quality of the photos, and the visibility of individuals within those photos.[19] Though early face recognition technologies could barely recognize a single face from a frontal view, technologies have now been developed to identify individuals in groups of people within images taken from diverse angles.[20] The CMU study discussed above showed that the photos available on Facebook, without so much as logging in, are sufficient to identify college students on a campus with approximately 30 percent success rate when using publicly available face recognition technology.[21]

B. Information Processed by Facebook's Photo Tag Suggest

In December 2010, Facebook introduced a new feature—called the "Photo Tag Suggest"—which uses face recognition technology and previously "tagged" photos to find users in newly uploaded photos.[22] While Facebook collects and retains a great deal of information about its users, this article focuses on the information that implicates face recognition technology.[23] That includes not only photos from which biometric data is extracted, but also all information displayed on a Facebook profile because, as explained below, by "tagging" a photo, the Photo Tag Suggest generates a hyperlink to the user's profile and all the information therein.

A Facebook profile contains a host of information about each user. Initially, Facebook "require[s a new user] to provide [her] name, email address, birthday, and gender."[24] Though not required, the user is also prompted to provide her religious belief, political views, and sexual orientation.[25] As the user goes through the process of friending other users (who may already be her friends, class mates, family, or colleagues offline), Facebook also retains a list of those friends.[26] A vast amount of communication between a user and her friends is also retained as the user makes "status updates," comments on friends' "walls," sends private messages, or chats with friends in real time.[27] Some of the personal information retained by Facebook is displayed on a user's profile and is visible to other users by default, unless the user changes her "privacy settings" to specify that the information should be visible to "friends only" or specific individuals.[28] Many users, however, do not understand or use these privacy settings.[29]

Facebook further collects photos uploaded by users and information about facial features when the users identify ("tag") themselves or others in those photos.[30] Facebook's photo collection contained around 100 billion photos by mid-2011 and was estimated to have increased by 6 billion photos each month.[31] According to Facebook, its users provide "more than 100 million tags" per day to that photo collection.[32] The uploaded photos may also provide Facebook with metadata, including the "time, date, and place" of a photo.[33] If a user uploads a photo from a mobile phone, Facebook may also know that user's physical location at that very instant.[34]

---

13 Given the many different technologies that have developed in this field (A. Abate et al., *2D and 3D Face Recognition: A Survey,* 28 Pattern Recognition Letters 14 (2007)), the description of the technology here is intended only as a general overview of the most basic steps in the face recognition process.

14 Stan Z. Li & Anil K. Jain, Handbook of Face Recognition 2-3 (Springer 2005).

15 *Id.*

16 *Id.*

17 *Id.*

18 *Id.*

19 Zhao & Chellappa, supra note 8, at 10.

20 *Id.* at 10-11.

21 Acquisti, Gross, & Stutzman, supra note 1.

22 Justin Mitchell, *Making Photo Tagging Easier,* The Facebook Blog, June 30, 2011, https://www.facebook.com/blog.php?post=467145887130 (last visited Nov. 12, 2011).

23 *Facebook Data Use Policy: Information We Receive and How It is Used,* Facebook, https://www.facebook.com/about/privacy/your-info#inforeceived (last visited Nov. 9, 2011).

24 *Id.*

25 Facebook, https://www.facebook.com (last visited Apr. 28, 2012).

26 *Id.*

27 *Id.*

28 Facebook Data Use Policy: Sharing and Finding You on Facebook, Facebook, https://www.facebook.com/about/privacy/your-info-on-fb#controlpost (last visited Nov. 9, 2011).

29 Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook,* 16 (2006), presented at Proceedings of Privacy Enhancing Technologies Workshop (PET) (finding that "among current members, 30% claim not to know whether FB grants any way to manage who can search for and find their profile, or think that they are given no such control"), available at http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf (last visited Feb. 12, 2012).

30 Facebook Data Use Policy: Information We Receive and How It is Used, *supra* note 23.

31 *Facebook Photo Trends [INFOGRAPHIC],* Pixable (Feb. 14, 2011), http://blog.pixable.com//2011/02/14/facebook-photo-trends-infographic/ (last visited Nov. 24, 2011).

32 Mitchell, *supra* note 22.

33 Facebook Data Use Policy: Information We Receive and How It is Used, *supra* note 23.

34 *Id.*

Facebook's Photo Tag Suggest implicates all of the personal information in a user's profile because it connects facial features detected in newly uploaded photos to that user's profile with a hyperlink. Users can manually tag a person in photos by marking a square around the person's face and providing the person's name. Once tagged, the name appears when hovering with the mouse over the tagged face in the photo. The name is also listed next to the photo as a hyperlink to the person's profile if she has a Facebook account. That profile may contain personal information, including email address, phone number, birthday, gender, religious belief, political views, sexual orientation, and countless personal status updates. The information in a user's profile may or may not be visible to a person clicking on the hyperlink depending on the selected privacy settings. Unless a user specifically opts out of being automatically identified in photos, Facebook uses tagged photos of that user to identify the user in newly uploaded photos.[35] Having identified the user, Facebook then suggests to the person uploading the photo that she tag the identified user in the photo, which results in a new hyperlink to the identified user's profile.[36]

Facebook's restriction that only a user's friends can use the Photo Tag Suggest to automatically identify her in photos does not necessary protect the user from abuse by automatic face recognition. In authoritarian countries, in particular, commentators have reported instances of dissidents being tortured to disclose their social network passwords.[37] The result is that behind another dissident's social network contact may be the very person this dissident needs most protection against. Even in democracies, there have been instances of schools, colleges, and employers demanding users' passwords to screen future employees and monitor students.[38] And for users who have some social network friends that they do not personally know offline, there is a risk that those friends are actually "socialbots."[39] A socialbot is software that is designed to behave like a human user and connect with users to inter alia gather their personal information.[40] Thus, for example, if a socialbot operator could get access to hundreds of college students' profiles, she could mirror the CMU experiment discussed above and instead use Photo Tag Suggest to identify those students on campus. She could then use elements of their offline and online activities to create elaborate identity theft schemes.[41]

II. Germany v. Facebook - Face to Face

When the Photo Tag Suggest was launched in Europe in June 2011 it provoked an immediate privacy outcry in the media.[42] Gerard Lommel, the Luxembourg member of the European Article 29 Data Protection Working Party, responded that there would be an investigation into its legality.[43] Further, the Hamburg Data Protection Commissioner Johannes Caspar argued that Photo Tag Suggest violates the EU Data Protection Directive and the German Federal Data Protection Act because it processes photos without obtaining specific consent from users.[44] He therefore demanded that Facebook bring the Photo Tag Suggest into compliance with the law or disable it.[45]

the Hamburg Data Protection Commissioner Johannes Caspar argued that Photo Tag Suggest violates the EU Data Protection Directive and the German Federal Data Protection Act because it processes photos without obtaining specific consent from users

In September 2011, Facebook entered into negotiations with the German federal government to sign a voluntary code of conduct regarding its privacy practices.[46] According to the Hamburg Data Protection Agency, Facebook initially considered a function that would make users aware of the Photo Tag Suggest and ask them to provide specific consent.[47] While it is unclear whether the Hamburg Data Protection Agency would have approved this solution, Facebook subsequently abandoned it and its negotiations with the federal government broke down.[48] On October 21, 2011, Mr. Caspar told Agence France-Presse that the agency would file an action against Facebook unless it proposed satisfactory changes to the Photo Tag Suggest by November 7th.[49] Facebook responded by proposing "a checkbox for users to accept terms and conditions

35 *Id.*

36 *Id.*

37 Adrian Blomfield, *Syria 'tortures activists to access their Facebook pages',* The Telegraph, May 9, 2011, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8503797/Syria-tortures-activists-to-access-their-Facebook-pages.html (last visited Feb. 16, 2012).

38 See, e.g., ACLU-MN files lawsuit against Minnewaska Area Schools, American Civil Liberties Union of Minnesota, Mar. 6, 2012, http://www.aclu-mn.org/news/2012/03/06/aclu-mn-files-lawsuit-against-minnewaska-area-schools (last visited Mar. 16, 2012); Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants' Facebook Passwords,* MSNBC, Mar. 6, 2012, http://redtape.msnbc.msn.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords (last visited Mar. 16, 2012).

39 John P. Mello Jr., *'Socialbots' Invade Facebook: Cull 250GB of Private Data,* PCWorld, Nov. 2, 2011, http://www.pcworld.com/article/243055/socialbots_invade_facebook_cull_250gb_of_private_data.html (last visited Feb. 11, 2012).

40 Id.

41 See, e.g., David D. Clark & Susan Landau, *Untangling Attribution,* in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (2010), available at http://www.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf (last visited Mar. 20, 2012).

42 Mitchell, *supra* note 22.

43 Stephanie Bodoni, *Facebook to be Probed in EU for Facial Recognition in Photos,* Bloomberg BusinessWeek, June 8, 2011, http://www.businessweek.com/news/2011-06-08/facebook-to-be-probed-in-eu-for-facial-recognition-in-photos.html (last visited Nov. 12, 2011).

44 Press Release, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Gesichtserkennungsfunktion von Facebook verstößt gegen europäisches und deutsches Datenschutzrecht (Aug. 2, 2011), available at http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html?tx_ttnews%5BbackPid%5D=170&cHash=b9607e92ef91d779f308acd01b7dd639 (last visited Nov. 14, 2011).

45 *Id.*

46 Press Release, Bundesinnenminister und Facebook verständigen sich auf stärkeren Schutz der Nutzer, Bundesministerium des Innern (Sept. 8, 2011), http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/09/facebook.html (last visited Nov. 14, 2011).

47 Hamburg DPA November 10 Press Release.

48 *See Id.*

49 *Germany Warns Facebook over Face-Recognition App,* Google News, Oct. 21, 2011, http://www.google.com/hostednews/afp/article/ALeqM5h6OE6S_Z3Noataserm-_OvN6bu9w?docId=CNG.4274462d8bc1dc67622b983a5b20b6da.171 (last visited Nov. 14, 2011).

and guidelines on data usage."[50] Mr. Caspar, however, remained unimpressed. First, he argued that "these guidelines on data usage [would not sufficiently] inform users about the face recognition function and the biometric database."[51] Second, the proposed consent would only be provided upon registration and would not apply to the over 20 million existing German Facebook members.[52] In a press release, Mr. Caspar announced that the agency was preparing an action to remedy Facebook's breach and to "ensure that new face recognition technologies [in the] future [are] implemented in a way that respects users' right of privacy and informational self[-]determination."[53]

Privacy is a firmly rooted concept under German law, which has developed a constitutional fundamental right to "informational self-determination."

To evaluate Mr. Caspar's argument that the Photo Tag Suggest violates the German Federal Data Protection Act, this article briefly reviews the EU Data Protection Directive as implemented by this Act and then analyzes the relevant provisions of the Act. This analysis will show that there is a strong argument that Photo Tag Suggest violates the Act by collecting biometric data and using it with other personal information, such as user names, contact information, and interests, without first obtaining users' informed and unambiguous consent.

A. The German Federal Data Protection Act Implements the EU Data Protection Directive

The European Union ("EU") requires "free movement of goods, persons, services and capital" between its member states to maintain an open internal market—which in turn necessitates free movement of data.[54] To facilitate free movement of personal data while protecting individuals' fundamental right to privacy, the EU sought to harmonize the national privacy protection laws in its member states.[55] The result was the EU Data Protection Directive ("Directive").[56] This Directive requires member states to enact legislation imposing procedural requirements upon the "automatic" processing of "personal data."[57] If a member state fails to enact national legislation to effectively "transpose" (i.e. implement) the Directive within three years, the Directive becomes "directly effective" within that state, allowing individuals to pursue an action against the state pursuant to the Directive.[58]

B. How Could the Photo Tag Suggest Violate German Law?

Privacy is a firmly rooted concept under German law, which has developed a constitutional fundamental right to "informational self-determination."[59] As early as in 1977, Germany adopted the Federal Data Protection Act ("BDSG")[60]—which has been praised as "the most perfectionist system of data privacy in the world."[61] As applied to face recognition technology, the BDSG likely requires that individuals give informed consent before their biometric data is collected or used and specific consent if particularly sensitive information is involved in the processing.

1. Users' Knowledge and Consent

The BDSG requires Facebook to seek users' written and informed permission for the "collection, processing and use of [their] personal data."[62] "Personal data" is "any information concerning personal or material circumstances of an identifiable or identified natural person."[63] The consent must be a "free decision" based upon information regarding the intended use of the information and, when appropriate, "the consequences of withholding consent."[64] Significantly, when consent is provided along with other written terms, it must be "distinguishable in its appearance."[65] Consent is not required, however, if the personal data is "generally accessible" and Facebook collects it merely for its "own commercial purposes." Even then, however, consent may still be required if the user "has a clear and overriding legitimate interest in [preventing the] processing or use."[66]

By applying the Photo Tag Suggest to photos, Facebook processes and uses personal information about individuals—such as their photos and names. Further, to the extent that the biometric data extracted

---

50 Lucian Constantin, *Germany Prepares to Sue Facebook Over Facial Recognition Feature,* PC World, Nov. 11, 2011, http://www.pcworld.com/businesscenter/article/243612/germany_prepares_to_sue_facebook_over_facial_recognition_feature.html (last visited Nov. 14, 2011).

51 Hamburg DPA November 10 Press Release, supra note 47.

52 *Id.*

53 *Id.*

54 Directive 1995/46, 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, Recital 3, 1995 O.J. (281) 31 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF (last visited Nov. 11, 2011).

55 *Id.*, Recital 9.

56 It is important to note that this Directive is in the course of being superseeded by an EU Data Protection Regulation that would be directly applicable in the EU Member States. 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, (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited Mar. 14, 2012).

57 European Parliament and Council Directive 95/46, *supra* note 54, Art. 3 and 4.

58 Case C-41/74, Van Duyn v Home Office, 1974 E.C.R. 1337; see also Consolidated Version of the Treaty on the Functioning of the European Union art. 288, Sep. 5, 2008, 2008 O.J. (C115) 47 ("A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods").

59 Entscheidungen des Bundesverfassungsgerichts (BVerfGE) (Federal Contitutional Court) Dec. 15, 1983, Neue Juristische Wochenschrift [NJW] 419, 1983 (Ger.).

60 Bundesdatenschutzgesetz [BDSG, Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, as amended Sept.14, 1994, BGBl. I at 2325, all subsequent quotations refer to an English translation of the Act available at http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile (last visited Dec. 1, 2011).

61 Schwartz, *supra* note 6, at 688; Inga Markovits, *Selective Memory: How the Law Affects What We Remember and Forget About the Past,* 35 L. & Soc'y Rev. 513, 522-523 (2001).

62 BDSG, §§ 4(1) and 4a(1).

63 *Id.* § 3(2).

64 *Id.* § 4a(1).

65 *Id.*

66 *Id.* § 28(1)(3).

from collected photos can be distinguished from those photos, Facebook is arguably also "collecting" new personal information. All of these actions require users' consent. It could be argued that consent is not required because users' tagged photos are already "generally accessible" and Facebook is processing them for its own purposes. However, many photos uploaded to Facebook have restricted access by virtue of privacy settings such that they would likely not be considered "generally accessible." Even for photos without restricted access, Facebook's interest in avoiding the consent requirement would be balanced against the users' interest in preventing the processing or use of the data. Given the possible intrusive uses of biometric data to identify users without their knowledge, that balancing may weigh in favor of requiring consent.

Second, one could imagine that the users' failure to opt out of the Photo Tag Suggest by adjusting their privacy settings constitutes implied consent to the collection and use of biometric data. However, the ability to opt out is insufficient for this purpose because the privacy settings for the Photo Tag Suggest do not look any different than the other privacy settings and thus are not "distinguishable in [their] appearance." Moreover, the Article 29 Working Party has opined that a user's failure to change the default settings in a social network should not constitute consent to a data use.[67] Rather, "[c]onsent must be given prior to the start of processing activities or before any new use of the data" so that users can make an "informed choice."[68] Opt-out consent is particularly flawed with respect to automatic face recognition because by the time a user opts out, the data has already been collected and potentially used to identify the person in new photos.

Significantly, Facebook has not actively notified its users that all of their personal information and biometric data derived from any photo in which they are tagged would be used to identify them in new photos. But when Facebook obtained personal information from users, it was required to inform them of "the purposes of [the] collection, processing or use."[69] This likely means that users should know specifically what biometric data is collected and from what photos. They should also know how long the data will be stored and who will have access to it in the meantime. Facebook further needs to explain in detail how it will aggregate and process the data and who will have access to the end results.

2. Collection of Biometric Data from Friends' Photos

What about when Facebook extracts a user's biometric data from photos uploaded by the user's friends? The BDSG tries to address that situation by requiring companies like Facebook to collect personal data directly from the user.[70] Yet Facebook may still collect data for its "commercial purpose" without the user's "participation" if (1) the data is "generally accessible";[71] or (2) if collecting it directly from the user would be too burdensome.[72] Crucially, data must nevertheless not be collected without the user's participation if there is a possibility that "overriding legitimate interests of the [user] would be adversely affected."[73]

It is hard to rationalize the collection of biometric data from friends' photos based on the premise that it would be too burdensome to obtain from the user. If the user makes it difficult for Facebook to collect biometric data from her own photos—by never uploading photos where her face can be identified or pixelating her photos so that Facebook's Photo Tag Suggest cannot extract biometric data from them—there is a possibility that the user has an "overriding legitimate interest" in maintaining anonymity.[74]

when consent is provided along with other written terms, it must be "distinguishable in its appearance

The more difficult question is whether biometric data from friends' photos can be considered "generally accessible." While the BDSG does not define the term "generally accessible" with respect to this exception, elsewhere in the statute the term is defined as data that "anyone can use, with or without prior registration, permission or the payment of a fee."[75] Clearly, friends' photos with restricted privacy settings would not qualify because they are not available to people without Facebook registration and even most of the users. However, photos without restricted privacy settings can be accessed by anyone. Indeed, the CMU researchers were able to use such photos without logging onto Facebook to identify roughly every third participant in the study mentioned above. However, even if such photos would be considered "generally accessible," Facebook's interest in using friends' photos to identify a person in new photos would be balanced against that person's interest in not being identified. On balance, the person's privacy interest may again outweigh Facebook's commercial interest because of the possible intrusive uses of biometrics—particularly as Facebook would still be able to use this data after seeking its users' permission.

3. Specific Consent When Facebook Is Used for Political Discourse

Facebook may also be required to obtain specific consent from users that provide particularly sensitive information on their profiles. For use of certain personal data, such as "political opinions," "religious or philosophical beliefs," and "sex life," the BDSG requires users to give prior consent that specifies the particular information in question.[76] Without specific consent, such data may only be processed if the company uses it "for [its] own commercial purposes [and the user] has manifestly made [it] public."[77] Facebook has enabled users to state their religious beliefs, political views, and sexual orientation in their profiles. To the extent that users chose to provide such information and do not make it "public" through their privacy settings, specific consent may be required before Photo Tag Suggest can generate hyperlinks to this information. Further, a user's failure to adjust the default settings perhaps would not be considered a "manifest" act to make that sensitive information "public." Therefore, the BDSG may require specific consent even if a user does not restrict access to the sensitive information she posts on her profile.

Continued on Page 28

67 Press Release, European data protection authorities clarify the notion of consent (Jul. 14, 2011) http://ec.europa.eu/justice/policies/privacy/news/docs/press_release%20opinion_on_consent_14072011.pdf (last visited Nov. 30, 2011); Opinion of the Article 29 Data Protection Working Party, 2011 O.J. (L 1197) 24, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (last visited Nov. 30, 2011).

68 *Id.*

69 BDSG, § 4(3). The notice must also provide (1) the identity of the person collecting the data and (2) the "categories of recipients" when the user does not expect the data to be "transferred to such recipients." *Id.*

70 *Id.* § 4(2).

71 *Id.* § 28(1)(3).

72 *Id.* § 4(2).

73 *Id.* §§ 4(2) and 28(1).

74 Adam Harvey, *CV Dazzle Camouflage from Computer Vision,* http://www.cvdazzle.com/ (last visited Mar. 15, 2012); Andrew W. Senior and Sharath Pankant, *Privacy Protection and Face Recognition* in Handbook of Face Recognition, *supra* note 14, at 681.

75 BDSG, § 10(5).

76 *Id.* §§ 3(9) and 4a(3).

77 *Id.* §§ 3(9), 4a(3), 4d(5), and 28(6)(2).

Continued from Page 9

Arguably the specific consent requirement does not add any privacy protection with respect to Facebook's Photo Tag Suggest because a user's Facebook friends can already view her political views on her profile. However, the reason this requirement may be needed is because there are at least two types of Facebook users: (1) those who use it as a virtual school yard or a lunch break room—simply to share everyday thoughts with their friends; and (2) users who state their political views (or other sensitive information), suggesting that they may use Facebook for a political cause.[78]

The more difficult question is whether biometric data from friends' photos can be considered "generally accessible."

The BDSG thus requires Facebook to provide the second group with additional notice and obtain consent specifically referring to the sensitive information at issue. Why does the second group need that additional notice? To see this, we can take the hypothetical example of a Facebook user who is a dissident in an oppressive regime. She states her political views on her profile and uses Facebook to plan future protests. Provided that she has not accidentally "friended" a government official who has created a fictitious account or tapped into another user's account, the government should not be able to use Facebook's Photo Tag Suggest to identify this dissident in photos. But if her friends were to upload photos of protests and use Photo Tag Suggest to identify her, a government official may be able to access those photos and see her name where she otherwise would have remained an anonymous face. The official may further be able to follow the hyperlink to her profile. Even if she already restricted her privacy settings to prevent the official from accessing the sensitive information in her profile, a tagged photo could give the official a clue as to where to find more information about the dissidents. The official may then try to hack into Facebook to obtain her personal information and contacts.[79] Additionally, the tagged photo may suggest to the official that the user participates in a group that organizes online, whereupon the government may try to disable her Internet access. Though Facebook would not be legally responsible for such actions taken by the oppressive government, the idea behind BDSG's requirements is to motivate Facebook to provide users with special notice when sensitive information is involved, so that users can take precautions as they see fit.

Privacy protection is particularly important as social networks are becoming channels for democratic discourse.[80] It could be argued that the problem demonstrated in the hypothetical above lies in the fact that Facebook is a general-purpose application that is not designed for political discourse and the BDGS's requirements are simply trying to fit a round peg into a square hole. If so, the solution would be to educate users not to use social networks for political purposes. But the very fact that Facebook is a general-purpose application may explain its potency for political action.[81] Facebook's executives have also emphasized its "key role in pushing demonstrators out of the closet and into Tahrir Square" during the Arab Spring in 2011.[82] Facebook's willingness to embrace this new role is admirable. However, some adjustments to its platform are necessary to ensure the safety of the people that rely on it for this purpose.

4. Overall Effectiveness of the German Law

The detailed requirements of user participation and informed consent—as well as specific consent requirements for sensitive information—allows Facebook users to regain some control over the immense amount of personal information that has migrated to the site. The BDSG achieves this without undue constraint on commercial interests and innovation. Facebook is, for example, not prohibited from introducing the Photo Tag Suggest. It simply must do it gradually and with full knowledge and permission from the users supplying their information.

This analysis of the BDSG with respect to Facebook's Photo Tag Suggest can also be extrapolated to online privacy more generally. The BDSG's provisions are effective because they are relatively specific as to what is required. They counter the typical pattern of online businesses to narrowly interpret ambiguous privacy laws in order to gain a competitive edge. That said, there remains room for improvement. The legislation could, for example, particularize the format of the required consent and the type of information that needs to be provided to the users. It could also be broken down by type of service and data, to eliminate any ambiguities.

C. Why Is the Hamburg Data Protection Agency Threatening Action Under German Law?

The press coverage of the German action against Facebook has been imbued with confusion about whether German law applies to Facebook and why the Hamburg Data Protection Agency—a German state, as opposed to federal, agency—is pursuing this action. To clear up that confusion, this article reviews the applicable choice of law and jurisdiction provisions.[83]

1. Does German Law Apply to Facebook?

The EU Data Protection Directive dictates that the transposing national legislation—such as the BDSG—should govern "the activities of [a company] on the territory of the Member State."[84] It further provides that if a company is "established on the territory of several Member States, [it] must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."[85] While Facebook has many offices in different EU countries, it also has an office in Hamburg, Germany.[86] The Directive therefore requires its operations in Germany to comply with German law.

There is a common misconception in the media that Facebook is only required to comply with Irish law that implements the Direc-

78 While the focus of this paper is on Facebook's face recognition feature, it should be noted that the BDSG would likely require Facebook to obtain specific consent from this second group of users with respect to many other functions that implicate sensitive information on their profiles.

79 For example, government security organizations or other organizations connected to the Syrian, Tunisian, Yemeni, and Iranian governments were believed to hack dissident websites and Facebook pages during the Arab Spring in 2011. Helmi Noman, *The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army,* Infowar Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/ (last visited Nov. 28, 2011).

80 Recommendation CM/Rec (2012) 4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services, Council of Europe, Apr. 4, 2012, https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383 (last visited Apr. 19, 2012).

81 See, e.g., Noam Cohen, *As Blogs Are Censored, It's Kittens to the Rescue,* New York Times, Jun. 21, 2009 (discussing Ethan Zuckerman's "Cute Cat Theory"), http://www.nytimes.com/2009/06/22/technology/internet/22link.html (last visited Dec. 1, 2011).

82 Brent Lang, *Facebook's Sheryl Sandberg: The Social Network Is a Force for Good,* The Wrap, Sept. 16, 2011, http://www.thewrap.com/media/column-post/facebooks-sheryl-sandberg-finding-jobs-spurring-arab-spring-31054 (last visited Nov. 29, 2011).

83 See Jonathan L. Zittrain, Jurisdiction 4 (Foundation Press 2005) (discussing the scope of choice of law and jurisdiction in cyberlaw).

84 European Parliament and Council Directive 95/45, supra note 54, Art. 4(1)(a).

85 Id.

tive.[87] The source of confusion appears to be that Facebook's international headquarters are located in Dublin, Ireland and that its terms of use provide a contractual relationship between Facebook's European users and Facebook Ireland Limited.[88] The notion that an Internet company must follow the law of the EU country where its headquarters are located comes from the EU Electronic Commerce Directive ("E-Commerce Directive").[89] Were the E-Commerce Directive applicable, the choice of law would depend on which Facebook office provides the relevant services to the German users.[90] Because Facebook's terms identify Facebook Ireland Limited as the contractual service provider for its European users, it is not clear that the Hamburg office would be found to be the provider of Facebook's services in Germany. This ambiguity may require an analysis of where Facebook has its "center of activities," which for the European market may well be in Ireland where the headquarters are located.[91] However, the jurisdiction analysis under the E-Commerce Directive is not applicable here. Rather, the E-Commerce Directive dictates that the choice of law for "the processing of personal data is solely governed by [the EU Data Protection] Directive," which as discussed above requires companies that are established in several EU countries to comply with all their data protection laws.[92] Thus, Facebook's Irish headquarters do not affect the applicability of BDSG to Facebook's processing of personal information in Germany.[93]

2. The Jurisdiction of the Hamburg Data Protection Agency

The Hamburg Data Protection Agency is further the appropriate agency to enforce the BDSG against Facebook's German operation because Facebook is a private entity with operations in Hamburg. While the BDSG tasks the Federal Data Protection Agency with monitoring the data practices of public entities, it requires local governments for the various Länder (i.e. states) to establish data protection agencies to oversee the *private* sector.[94] Accordingly, section 24 of the Hamburg Data Protection Act provides that that the Hamburg Data Protection Agency has the authority to monitor private entities' compliance with the BDSG in Hamburg.[95] In the course of its monitoring, this agency may require entities to provide information within a specified period of time and may inspect their facilities and business records during normal office hours.[96] The agency may also order a company to cure violations of the BDSG and impose fines.[97] If the company fails to comply with an order within a reasonable time and the violation involves a serious breach of privacy, the agency may enjoin the processing of data until the violation is remedied.[98] Given that Facebook is a private entity with an office in Hamburg, the Hamburg Data Protection Agency has jurisdiction to inspect its operation and may file an action if it finds a violation.

when used in social networks, face recognition technology is also capable of connecting an otherwise anonymous face to a vast amount of personal information

III. Conclusion

Social networks provide people with an incredibly valuable tool for social interaction. In a fast-paced globalized world, they allow users to stay in touch with their friends and family in a meaningful way regardless of their geographical location. Yet Facebook and other social networks have a commercial interest in aggregating users personal information to sell advertising.[99] Face recognition technology, in particular, serves this function by simplifying the process of uploading and tagging many photos.[100] However, when used in social networks, face recognition technology is also capable of connecting an otherwise anonymous face to a vast amount of personal information. Given that this process implicates an individual's right to information self-determination, it is thoroughly regulated by the German Federal Data Protection Act. This law is enforceable by the Hamburg Data Protection Agency that has jurisdiction over all private entities in Hamburg and it applies to Facebook's data uses in Germany even though Facebook's headquarters are located in Dublin. As the Hamburg Data Protection Agency is still to file its threatened action against Facebook, we may soon discover the true force of this law as applied to face recognition technology.

Yana Welinder is an LL.M. Candidate at Harvard Law School.[1]

1 A much earlier version of this article was submitted in conjunction with a seminar and the author would like to thank Prof. Herbert Burkert for his thoughtful comments on that draft. The author would also like to thank Prof. Daria Roithmayr, Prof. Jonathan Zittrain, Prof. Yochai Benkler, Angelica Eriksson, and Ryan Budish for their invaluable comments on earlier versions of this article. Any errors and omissions are the author's own.

86 Factsheet, Facebook, https://www.facebook.com/press/info.php?factsheet (last visited Nov. 11, 2011).

87 See, e.g., Pamela Duncan, *Commissioner to Begin Facebook Audit,* IRISH TIMES, Sept. 28, 2011, http://www.irishtimes.com/newspaper/breaking/2011/0928/breaking60.html (last visited Nov. 11, 2011); Tiffany Kaiser, FTC, *Irish Data Protection Commissioner Probe Facebook Over Privacy Concerns,* DAILYTECH, Sept. 30, 2011, http://www.dailytech.com/article.aspx?newsid=22889 (last visited Nov. 15, 2011); *Data Commissioner to begin Facebook audit,* RTE NEWS, Sept. 28, 2011, http://www.rte.ie/news/2011/0928/facebook.html (last visited Nov. 15, 2011).

88 Press Release: Facebook, Facebook to Establish International Headquarters in Dublin, Ireland (Oct. 2, 2008), available at https://www.facebook.com/press/releases.php?p=59042 (last visited Nov. 11, 2011); *Terms of Use,* Facebook, Section 18, https://www.facebook.com/terms.php (last visited Nov.11, 2011).

89 Council Directive E-Commerce Directive 2000/31, 2000 O.J. (178) 1 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF (last visited Nov. 11, 2011).

90 The E-Commerce Directive provides that "[e]ach Member State shall ensure that the information society services provided by a service provider established on its territory comply with . . . national provisions." *Id.* Art. 3. "[T]he concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period." *Id.* at Recital 18. When "a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided." *Id.*

91 If "it is difficult to determine from which of several places of establishment a given service is provided, ... the place where the provider has the cent[er] of his activities relating to this particular service" is deemed to be the "place of establishment." *Id.*

92 European Parliament and Council Directive 95/46, *supra* note 54, Recital 14.

93 To be sure, Facebook's data processing in Ireland does fall under Irish jurisdiction and the Irish Data Protection Agency is also investigating the legality of the Photo Tag Suggest. Carl Franzen, *Facebook Making Changes to Avoid Irish Fines,* TPM (Nov. 14, 2011, 3:20 PM), *http://idealab.talkingpointsmemo.com/2011/11/facebooks-irish-privacy-audit-results-due-before-2012.php* (last visited Nov. 15, 2011).

94 BDSG, Section 38(6).

95 Hamburgisches Datenschutzgesetz [HmbDS , Hamburg Data Protection Act], Jul. 5, 1990, GVBI. Hamburg, § 24, available at http://www.datenschutz-hamburg.de/uploads/media/Hamburgisches_Datenschutzgesetz__HmbDSG_.pdf (last visited Dec. 1, 2011).

96 BDSG, §§ 38(3) and (4).

97 *Id.* § 38(5).

98 *Id.*

99 Ballmer: They Paid How Much For That?, Bloomberg BusinessWeek, Oct. 23, 2006, http://www.businessweek.com/magazine/content/06_43/b4006066.htm (last visited Nov. 15, 2011).

100 Mitchell, *supra* note 22.