Articles

Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field

By Anne-Marie Zell[*]

Abstract

With the negotiation of its Data Protection Regulation, the European Union seeks to reform an outdated set of laws that has failed to address the evolving data protection challenges inherent in new technologies such as social networks, e-commerce, cloud computing, and location-based services. This article addresses the forthcoming Data Protection Regulation as well as the current state of data protection law in the EU, with a particular focus on Germany. The first part of the article examines Germany's robust data protection framework and the EU's existing authority. The article then raises key issues related to data protection in Germany and the EU—namely, discrepancies in data protection standards and enforcement among EU Member States—as illustrated by recent, high profile cases involving household names like Facebook, Apple, Google, and Amazon. Through this analysis, the article attempts to explain how and why companies doing business in Germany, but established in other EU Member States, are subject to less stringent data protection standards than German companies. Lastly, the article synthesizes the issues in debate with regard to the draft Data Protection Regulation and offers perspectives on what the Regulation could and should mean for data protection in the EU.

[*] Fellow, Robert Bosch Fellowship for Young American Leaders (2012-2013); Juris Doctor, William & Mary Law School (2006). This article was sponsored by the Robert Bosch Foundation, Stuttgart, Germany, with additional support from the Otto Group GmbH, Hamburg, Germany.

A. Introduction

The Federal Republic of Germany maintains one of the strongest data privacy protection frameworks in the European Union and the world,[1] the cornerstones of which are the *Bundesdatenschutzgeset*z (Federal Data Protection Act)[2] and the *Telemediengesetz* (Telemedia Act).[3] One might say this is a boon to German citizens, who on the whole highly value online privacy and are proactive in voicing disapproval of data practices that may infringe on that privacy.[4] However, as the recent Facebook "Real Names Policy" case[5] has shown, the EU Data Protection Directive[6]—the current EU data protection law—has rendered Germany unable to apply these stringent standards equitably. Companies like Facebook that are established in at least one EU Member State other than Germany are able to circumvent German law even as they direct their products and services to German consumers, and as German companies remain subject to those laws.[7] Thus, the unintentional effect of German and EU data protection laws has been to create an unequal playing field, penalizing German companies that choose to retain headquarters, data processing, and other core functions within the country and encouraging companies with fewer German ties to forum shop for EU Member States with more lenient standards.[8] To

[1] *See, e.g.*, *Surveillance Monitor 2011: Assessment of Surveillance across Europe*, PRIVACY INTERNATIONAL (2011), https://www.privacyinternational.org/reports/surveillance-monitor-2011-assessment-of-surveillance-across-europe (noting Germany's data protection framework is "amongst the best in the world . . . ."); *National Privacy Ranking 2007 – Leading Surveillance Societies Around the World*, PRIVACY INTERNATIONAL (2007), *available at* https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/phrcomp_sort_0.pdf (assigning Germany a higher data privacy ranking in the category of data-sharing than all other EU as well as non-EU countries surveyed).

[2] Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], repromulgated Jan. 14, 2003, BUNDESGESETZBLATT, Teil I [BGBL. I] at 66, last amended by Gesetz [G], Aug. 14, 2009, BGBL. I at 2814 [hereinafter BDSG].

[3] Telemediengesetz [TMG] [Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT, Teil I [BGBL. I] at 179, last amended by Gesetz [G], May 31, 2010, BGBL. I at 692, at art. 1.

[4] *See supra* note 1.

[5] Press Release, *OVG Schleswig-Holstein: For Facebook Germany Data Protection Law Does Not Apply*, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) (Independent State Center for Data Protection Schleswig-Holstein), (Apr. 24, 2013), *available at* https://www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg-en.htm.

[6] EC Directive 95/46/EC of 24 October 1995, O.J. L 281.

[7] *See supra* note 5.

[8] Konrad Lischka & Christian Stöcker, *Data Protection: All You Need to Know about the EU Privacy*, SPIEGEL ONLINE, 18 Jan. 2013, http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html (surmising the new Data Protection Regulation could "lead to . . . corporations choos[ing] . . . European headquarters based on the strength, or lack thereof, of data protection supervision in that country" and noting "competition between countries in attracting companies to locate their offices there has already been a phenomenon in the EU for some time now").

add to the complexity, on 25 January 2012 the EU released a draft of the forthcoming Data Protection Regulation, which is to supersede the current EU Data Protection Directive as well as German data protection laws.[9]

In view of the foregoing, this article will first examine the current German and EU data protection laws, providing a summary of the relevant legal authority. The article will then raise key issues related to data protection in Germany and the EU as illustrated through recent, high profile cases. Finally, with regard to the draft EU Data Protection Regulation, the article will contemplate how the EU might curtail current and prevent future forum shopping and uphold fair competition.

B. Relevant Authority

The EU laws on data protection currently in force, primarily the Data Protection Directive (DPD)[10] and the E-Privacy Directive,[11] govern the collection and handling of personal data throughout the EU and seek to harmonize the data protection policies of Member States.[12] These EU laws prescribe only a threshold level of data protection;[13] thus, the national laws of some Member States, such as Germany, guarantee a higher level of data protection.[14] As noted above, in many cases Member States with stricter standards are prohibited under EU law from applying national law (*e.g.*, the *Bundesdatenschutzgeset*z) to companies from other Member States.[15] The EU laws that do apply are often outdated and insufficient. Enacted in 1995, the EU's DPD does not adequately address present-day, much less

[9] *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) [hereinafter "Data Protection Regulation"].

[10] Directive 95/46, 1995 O.J. (L 281) [hereinafter "DPD"] (EC).

[11] Directive 2002/58, 2002 O.J. (L 201/37) [hereinafter "E-Privacy Directive"] (EC).

[12] The EU acknowledges there is a need to "ensure that the fundamental right to data protection is consistently applied." *Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme*, at 3, COM (2010) 171 final (Apr. 20 2010).

[13] For example, the EU's Working Time Directive, 2003/88/EC, gave workers the right to work no more than 48 hours per week; France passed stricter regulations, limiting working hours to 35 hours per week; *See* French Labour Code, Art. L.212-1 et seq.; Heidi Blake, *The EU Working Time Directive in Detail*, THE TELEGRAPH, June 9 2010; *See also*, infra Part B.II. for a discussion of the differences between EU directives and regulations.

[14] *See, e.g.*, Dr. Nils Christian Haag, *Court: German Data Protection Law is Not Applicable to Facebook*, PRIVACY EUROPE, Feb. 15 2013, http://www.privacy-europe.com/blog/court-german-data-protection-law-is-not-applicable-for-facebook.

[15] DPD, *supra* note 10, at Art. 4(1)(a).

prospective, data protection challenges.[16] Increased internet use combined with new technologies—for example, social networks, e-commerce, cloud computing, and location-based services such as GPS—presents data collection issues the DPD did not foresee.[17]

I. Federal Republic of Germany

1. Bundesdatenschutzgesetz (Federal Data Protection Act)

The German data protection law—the *Bundesdatenschutzgesetz* (BDSG)—affords German citizens a high level of data protection.[18] The law was enacted in 2003 and most recently amended in 2009.[19] It aims to protect individuals' privacy and guard against the mishandling of personal data.[20] To that end, the law specifically targets the "collection, processing and use" of personal data.[21]

The BDSG applies to certain public[22] and private bodies.[23] "Private bodies" are defined as "natural or legal persons, companies and other private-law associations."[24] With regard to the application of the law to these private bodies, the BDSG provides as follows:

> This Act shall apply to the collection, processing and use of personal data by . . . private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection,

[16] *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st* Century, at 3, COM (2012) 9 final (Jan. 25 2012) (noting the DPD "was adopted 17 years ago when the internet was in its infancy).

[17] *Id*. at 2.

[18] *See supra* note 2.

[19] *Id*.

[20] BDSG, *supra* note 2, § 1. The BDSG defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)." *Id.* § 3.1.

[21] *Id.* § 2.

[22] *Id.* § 2.1-2.

[23] *Id.* § 2

[24] *Id.* § 2.4.

> processing or use of such data is effected solely for personal or family activities.[25]

However, the BDSG exempts private bodies "*located in another Member State of the European Union or in another state party to the Agreement on the European Economic Area*" so long as the "*collection, processing or use [of personal data] is [not] carried out by a branch in Germany*."[26] This means, in effect, that so long as a corporation doing business in Germany is headquartered in another Member State (or qualifying member of the EEA)[27] and defers the collection, processing, and use of personal data to a location outside of Germany, the corporation's handling of personal data, including that of German citizens, is not subject to the BDSG.

As for substantive provisions, the BDSG has three notable attributes: (1) it requires data controllers[28] to obtain express consent from an individual for the processing, collecting, and use of the individual's personal data;[29] (2) it contains a "list privilege" exception, with conditions that data controllers can fairly easily meet;[30] and (3) it requires data controllers notify affected individuals of data breaches, and conditions this notification requirement on a single instance of breach.[31]

1.1 Express Consent

With regard to consent, the BDSG prescribes that personal data may only be collected, processed, or used if the individual, the "data subject," expressly consents.[32] The intent of the express consent requirement is to enhance the data subject's ability to make informed and free choices.[33] The BDSG states, "Consent shall be effective only when based on the

---

[25] *Id.* § 2.3.

[26] *Id.* § 5 (emphasis added).

[27] The EEA is comprised of EU Member States plus three of four European Free Trade Association (EFTA) members, namely, Iceland, Norway, and Lichtenstein, and establishes a single market between the parties, known as the "internal market." The fourth member of the EFTA that is not a party to the EEA is Switzerland. *See* Agreement on the European Economic Area, at 3–522, 1994 O.J. (L 1).

[28] A "controller" is defined as "any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same." BDSG, *supra* note 2, § 3.7.

[29] *Id.* §§ 4.1, 4(a).1

[30] *Id.* § 28.

[31] *Id.* § 42(a).

[32] *Id.* § 4.1.

[33] *Id.* § 4.1.

data subject's free decision."[34] Furthermore, for the consent to be valid, the data subject must have been properly informed as to the "purpose of the collection, processing or use."[35] Upon the data subject's request, the data controller must inform the data subject of the consequences of withholding consent.[36] Barring "special circumstances," the consent must be in writing.[37]

If the data controller is collecting special types of personal data, as described in Section 3.9 of the BDSG—race, ethnicity, political opinions, religious or philosophical beliefs, union membership, health, or sex life[38]—the data controller must expressly refer to that data in the request for consent.[39]

1.2 List Privilege Exception

The "list privilege exception" refers to a clause that allows the "processing or use of personal data for the purposes of advertising or trading in addresses" where the data subject has given consent and the data "consists of lists or other summaries of data from groups of persons which are limited to the data subject's membership of this group, his/her occupation, name, title, academic degrees, address and year of birth."[40] The conditions are fairly easy for data controllers to meet, which means use of a data subject's name, birth year, job, level of education, and address are usually fair game for advertising purposes, and for transferring or selling to other companies.[41]

The use of this list data by the data controller or the transfer or sale to another company for advertising purposes is conditioned on the data controller first obtaining the data subject's consent. However, the data controller may transfer or sell this list data for advertising purposes *without* obtaining the data subject's consent if the data controller stores records of the data transfer—specifically, the data's origin and the recipient of the

[34] *Id.*

[35] *Id.* § 4(a).1.

[36] *Id.*

[37] *Id.*

[38] *Id.* § 3.9.

[39] *Id.* § 4(a).3.

[40] *Id.* § 28.3.

[41] Jorg Rehder & Mauricio Paez, *Germany Strengthens its Data Protection Act and Introduces Data Breach Notification Requirement,* 16 BNA INT'L WORLD DATA PROTECTION REP. 1 (2010), http://www.jonesday.com/germany-strengthens-data-protection-act-introduces-data-breach-notification-requirement-10-26-2009/.

transfer—for two years and any advertising clearly states which company originally collected the data.[42]

Likewise, under the list privilege exception the data controller may use data *without* consent from the data subject where the "processing or use is necessary" for (1) the data controller's own advertising offers (based on data collected either for the purpose of satisfying a legal or quasi-legal obligation or from "generally accessible sources" like public directories);[43] (2) advertising related to the data subject's job or work address;[44] or (3) solicitation of charitable donations.[45]

1.3 Data Breach Notification

The data breach notification required by the BDSG applies to four categories of personal data, one of which, for example, is bank account or credit card information.[46] If the personal data stored by a data controller has been "unlawfully transferred or otherwise unlawfully revealed to third parties" and there is a "threat of serious harm to the data subject's rights or legitimate interests," the data controller must notify both the supervisory authority and the data subject "without delay."[47] Notably, there is no threshold requirement that the data breach compromise a certain number of accounts; this means breach of a single account would trigger the notification requirement, so long as the breach posed a threat of serious harm to the data subject.[48]

When notifying a data subject of a breach, the data controller must "describe the nature of the unlawful access and include recommendations for measures to minimize possible harm."[49] When notifying the supervisory authority, the data controller must set forth the "possible harmful consequences of the unlawful access" and describe remedial measures the data controller has undertaken.[50]

---

[42] BDSG, *supra* note 2, §§ 28.3.3, 34.1(a).

[43] *Id.* §§ 28.1.1, 28.3.1.

[44] *Id.* § 28.3.2.

[45] *Id.* § 28.3.3. *See also supra* note 41.

[46] The other three categories are 1) "special types of personal data" as described in Section 3.9, including data on race, ethnicity, political opinions, religious or philosophical beliefs, union membership, health, or sex life. 2) "personal data subject to professional secrecy," and 3) "personal data related to criminal offences or administrative offences or the suspicion [thereof]." BDSG, *supra* note 2, § 42(a).

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

2. Gesetz gegen den unlauteren Wettbewerb (UWG) (Act against Unfair Competition)

The German unfair competition law, the *Gesetz gegen den unlauteren Wettbewerb* (UWG), came into force in July 2004.[51] The purpose of the law is to protect "competitors, consumers and other market participants against unfair commercial practices" and "the interests of the public in undistorted competition."[52]

The UWG outlaws unfair commercial practices and cites several examples of prohibited behavior, including, *inter alia*, when a person (1) "uses commercial practices that are suited to impairing the freedom of decision of consumers or other market participants through applying pressure . . . ."; [53] (2) "uses commercial practices that are suited to exploitation of a consumer's mental or physical infirmity, age, commercial inexperience, credulity or fear, or the position of constraint to which the consumer is subject";[54] (3) "conceals the advertising nature of commercial practices";[55] (4) "deliberately obstructs competitors;"[56] and (5) "infringes a statutory provision that is also intended to regulate market behavior in the interest of market participants."[57] The UWG also prohibits misleading commercial practices[58] and "unconscionable pestering,,"[59] and places limits on comparative advertising.[60]

The UWG's provision on unconscionable pestering requires advertisers to obtain prior express consent from potential recipients before sending them emails with advertising content.[61] The provision states, "Unconscionable pestering shall always be assumed in the case of . . . advertising using an automated calling machine, a fax machine or electronic

[51] *Gesetz Gegen den Unlauteren Wettbewerb* [UWG] [Act Against Unfair Competition], Mar. 3 2010, BUNDESGESETZBLATT, Teil I [BGBL. I], last amended by Gesetz [G], Mar. 3, 2010, BGBL. I at 254 [hereinafter UWG].

[52] *Id.* § 1.

[53] *Id.* § 4.1.

[54] *Id.* § 4.2.

[55] *Id.* § 4.3.

[56] *Id.* § 4.10.

[57] *Id.* § 4.11.

[58] *Id.* §§ 5, 5(a).

[59] *Id.* § 7.

[60] *Id.* § 6.

[61] *Id.* § 8.

mail without the addressees prior express consent."[62] Advertisers in Germany rely on a "double opt-in" process that several German courts have endorsed.[63] When agreeing to receive advertising email, the recipient first must affirmatively check a box.[64] Then, the advertiser must send an email with a confirmation link to the recipient (the "Check-Mail"), and the recipient must click through the link.[65] Only then is the advertiser allowed to send advertising emails to the recipient. The confirmation link is meant to ensure that people are not falsely enrolled by someone else.[66]

Under the UWG, a firm may sue a competitor that violates either section 3 (Prohibition of Unfair Commercial Practices) or section 7 (Unconscionable Pestering) for "elimination" and "in the event of the risk or recurrence, for cessation and desistance."[67] However, the firm must first send the offending party a warning letter, the *Abmahnung*, and give the party a chance to remedy the issue before filing suit.[68]

3. Telemediengesetz (Telemedia Act)

The *Telemediengesetz* (TMG) regulates the provision of online services such as websites and email.[69] The TMG applies to "all electronic information and communications services, to the extent that they are not telecommunications services[70] . . . or broadcasting . . . ."[71]

---

[62] *Id.* § 8.2(3).

[63] Bundesgerichtshof [BGH - Federal Court of Justice], Case No. I ZR 164/09 (Feb. 10, 2011), http://dejure.org/dienste/vernetzung/rechtsprechung?Text=I%20ZR%20164/09; Landgericht [LG (Berlin) - Regional Court], Case No. 15 O 346/06 (Jan. 23, 2007), http://dejure.org/dienste/vernetzung/rechtsprechung?Text=15%20O%20346/06; Amtsgericht [AG – (Berlin-Mitte) - Local Court], Case No. 21 C 43/08 (June 11, 2008), http://dejure.org/dienste/vernetzung/rechtsprechung?Text=21%20C%2043/08; Landgericht [LG (Essen) - Regional Court], Case No. 4 O 368/08 (Apr. 20, 2009), http://dejure.org/dienste/vernetzung/rechtsprechung?Text=4%20O%20368/08. *But see*, Oberlandesgericht [OLG - (München) Higher Regional Court], Case No. 29 U 1682/12 (Sept. 27, 2012), http://dejure.org/dienste/vernetzung/rechtsprechung?Text=29%20U%201682/12 (holding the "Check-Mail"—the initial email confirming an individual's consent to receive advertising email—of the double opt-in method can constitute spam).

[64] Tim Englehardt, *Is Double Opt-In Dead?*, GERMAN IT LAW BLOG, Nov. 26, 2012, http://germanitlaw.com/?p=902.

[65] *Id*.

[66] *Id*.

[67] UWG, *supra* note 51, § 8.

[68] *Id.* § 12.1.

[69] *See supra* note 3.

[70] Defined as "services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks

One aim of the TMG is to streamline and enhance data protection in the realm of online services.[72] Enacted in 2007, the TMG consolidated and replaced several German laws: the *Telemedienstegesetz* (Teleservices Act),[73] the *Mediendienste-Staatsvertrag* (Federal Media Services Treaty),[74] and the *Teledienstedatenschutzgesetz* (Teleservices Data Protection Act).[75]

The TMG adheres to a "country of origin principle."[76] This means that online service providers "established"[77] within Germany are subject to the TMG, even when those services are offered in other Member States.[78] With respect to online service providers established in other Member States, but directing offers and services toward German consumers, the TMG simply states the "free movement" of those services is unrestricted: "[F]ree movement of telemedia services which are commercially offered or provided in the Federal Republic of Germany by service providers which are established in another state within the scope of [the EU Directive on Electronic Commerce] is not restricted."[79]

With regard to commercial communications, the TMG requires that service providers clearly identify the sender of the message and that the nature of the message is

---

used for broadcasting." *Telekommunikationsgesetz* [TKG] [Telecommunications Act], June 22, 2004, BUNDESGESETZBLATT, Teil I [BGBL. I] at 1190, last amended by Gesetz [G], 3 May 2013, BGBL. I at 958, art. 1, § 3.24.

[71] TMG, *supra* note 3, § 1.1.

[72] *See* Karen Sokoll & Christoph Enaux, *Germany—New Telemedia Act Introduced*, LINKLATERS: TECHNOLOGY, MEDIA & TELECOMMS. News, Mar. 24, 2007, http://www.linklaters.com/Publications/Publication1403Newsletter/PublicationIssue20070324/Pages/PublicationIssueItem2217.aspx.

[73] *Gesetz über die Nutzung von Telediensten (Teledienstegesetz)* [Teleservices Act], July 22, 1997, BUNDESGESETZBLATT, Teil I [BGBL. I] at 1870.

[74] *Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag)* [Federal Media Services Treaty], Jan. 20 – Feb. 12, 1997, ratified June 19, 1997, NIEDERSACHSEN GESETZ- UND VERORDNUNGSBLATT [GVBL.] 280.

[75] *Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz)* [Teleservices Data Protection Act], July 22, 1997, BUNDESGESETZBLATT, Teil I [BGBL. I] at 1870. *See, e.g.,* Henning Krieg, *German Telemedia Act Introduces New Rules for New Media*, BIRD & BIRD, Mar. 30, 2007, http://www.twobirds.com/English/News/Articles/Pages/2007/German_Tele_Media_Act_new_rules.aspx.

[76] TMG, *supra* note 3, § 3.

[77] The TMG defines "established service provider" as "every provider who uses who uses a fixed facility for an indefinite period to offer or provide telemedia on a commercial basis" and notes further that "the location of the technical facility alone does not determine that the provider is established." *Id*. § 2.2.

[78] *Id*. § 3.1.

[79] *Id*. § 3.2.

commercial.[80] Service provides must also clearly identify any promotional offers or advertising.[81] For example, a game may not serve as an advertising tool unless clearly identified as such.[82]

The collection of personal data in connection with the provision of telemedia services only is allowed if expressly provided for by the TMG or other legislation or if the individual has consented.[83] Additionally, the service provider may not condition use of the telemedia service upon consent if the individual cannot reasonably access the service through another means.[84] When collecting personal data, the TMG requires the service provider to alert the individual as to the "nature, scope and purpose of the collection and use of personal data . . . ."[85]

Under the TMG, an individual has the right to (1) terminate telemedia service at any time;[86] (2) have his or her personal data immediately deleted following termination of the telemedia service;[87] (3) use telemedia service with no disclosure of use to third parties;[88] and, importantly, (4) pseudonymous use of telemedia services.[89]

With regard to pseudonymous use, the TMG states, "The service provider must enable the use of telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable. The recipient of the service is to be informed about this possibility."[90] A service provider may not cobble together user profiles and other details to uncover the identity of someone using a pseudonym.[91] Nevertheless, service providers are allowed to create anonymous profiles for pseudonym users under certain circumstances:

---

[80] *Id*. §§ 6.1.1–2.

[81] *Id*. §§ 6.1.3–4.

[82] *Id*. § 6.1.4.

[83] *Id.* § 12.1.

[84] *Id*. § 12.3.

[85] *Id*. § 13.1.

[86] *Id*. § 13.4.1.

[87] *Id*. § 13.4.2.

[88] *Id*. § 13.4.3.

[89] *Id.* § 13.6.

[90] *Id*. § 13.6.

[91] *Id*. § 13.4.6.

> For the purposes of advertising, market research or in order to design the telemedia in a needs-based manner, the service provider may produce profiles of usage based on pseudonyms to the extent that the recipient of the service does not object to this. The service provider must refer the recipient of the service to his right of refusal pursuant to Sub-section 13 No. 1. These profiles of usage must not be collated with data on the bearer of the pseudonym.[92]

This means service providers can use anonymous profiles of pseudonym users to research market trends and support advertising strategy.[93] However, the data subject has a right to object to the profile creation and the service provider must bring this right to the data subject's attention.[94]

II. European Union

The Treaty on the Functioning of the European Union (the Treaty of Rome or TFEU)[95] and the Treaty on the European Union (the Maastricht Treaty or TEU)[96]—both as amended by the Lisbon Treaty[97]—and the Charter of Fundamental Rights of the European Union[98] together form the foundation of the European Union. The EU utilizes several legal instruments to further the objectives of these foundational agreements.[99]

As modeled by the Data Protection Directive, a "directive" applies to Member States, as opposed to EU citizens,[100] and sets forth a legal framework to be implemented by the

[92] *Id*. § 15.3.

[93] *Id*.

[94] *Id*.

[95] Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter "TFEU"].

[96] Consolidated Version of the Treaty on European Union, Oct. 26, 2012, 2012 O.J. (C 326) 13 [hereinafter "TEU"].

[97] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter "Lisbon Treaty"].

[98] Charter of Fundamental Rights of the European Union, Mar. 30, 2010, 2010 O.J. (C 83) 2 [hereinafter "Charter"].

[99] *Regulations, Directives, and Other Acts*, EUROPEAN UNION, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm.

[100] TFEU art. 288. *See also*, *supra* note 10.

Member States through a process known as "transposition."[101] Each Member state promulgates its own laws to effect implementation of a directive.[102] A "regulation" on the other hand, such as the forthcoming Data Protection Regulation, is immediately binding upon all EU citizens when enacted and there is no need for Member States to pass implementing legislation.[103] Therefore, a regulation is likely to be more consistent in its application across Member States than a directive.[104] An "opinion," such as those issued by the EU Commission, Council, Parliament, or Article 29 Data Protection Working Group, is a non-binding analysis.[105] In contrast, a "decision" is binding generally or, if addressed, only on the addressees.[106]

1. Charter of Fundamental Rights of the European Union

At the EU level, the Charter of Fundamental Rights of the European Union (the "Fundamental Rights Charter") guarantees an individual's right to protection of his or her personal data.[107] The Fundamental Rights Charter, which was drafted in 2000 and came into force in 2009, references the EU's dual goals of "development of . . . common values while respecting the diversity of the cultures and tradition of the peoples of Europe" and "ensur[ing] free movement of persons, services, goods and capital . . . ."[108] The EU's focus on free movement stems from its efforts to create a single economic market within the EU—the "Single Market" or, in German, "der Binnenmarkt."

In regard to data protection, the Fundamental Rights Charter declares, "Everyone has the right to the protection of personal data concerning him or her."[109] The Fundamental Rights Charter further clarifies what constitutes appropriate handing of personal data: "Such data must be processed fairly for specified purposes and on the basis of the consent of the

[101] Transposition is "a process by which the European Union's member states give force to a directive by passing appropriate implementation measures." *Transposition (law)*, WIKIPEDIA, Mar. 9, 2013, http://en.wikipedia.org/w/index.php?title=Transposition_(law)&oldid=543106078.

[102] *See supra* note 100.

[103] *Id.*

[104] *See supra* note 13; *see also*, W. Kuan Hon, et. al, *Data Protection Jurisdiction and Cloud Computing—When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3*, 26 INT'L REV. OF LAW, COMPUTERS & TECH. 129, 135 (2012).

[105] TFEU art. 288.

[106] *Id.*

[107] Charter art. 8.

[108] *Id.* at art. 391.

[109] *Id.* at art. 8.1.

person concerned or some other legitimate basis laid down by law. . . ."[110] Notably, the Fundamental Rights Charter does not specify whether the consent must be express versus implied.[111] The Fundamental Rights Charter also secures an individual's "right of access to data which has been collected concerning him or her," as well as the right to correct any misinformation.[112] Finally, the Fundamental Rights Charter notes that an independent authority will oversee compliance.[113] Although not noted in the Charter, the independent authority for the EU is the European Data Protection Supervisor (EDPS).[114]

2. Treaty on the Functioning of the European Union (TFEU) as Amended by the Lisbon Treaty

The Lisbon Treaty between the Member States came into force in 2009, amending both the TFEU and the TEU.[115] The Lisbon Treaty abolished the European Community's system of three legal pillars and consolidated the pillars into one legal entity under the heading of the EU.[116] Like the Fundamental Rights Charter, the TFEU guarantees an individual's right to the protection of his or her data. [117] Article 16 of the TFEU declares, "Everyone has the right to the protection of personal data concerning them."[118] This provision is the legal basis for the EU's adoption of the forthcoming Data Protection Regulation.[119]

3. Data Protection Directive

The objective of the Data Protection Directive (DPD) mirrors that of the Fundamental Rights Charter and is likewise twofold—first, to protect the "fundamental rights and freedoms" of individuals, "in particular their right to privacy with respect to the processing of data," and, second, to enhance the "free flow of personal data between Member States."[120] The Directive was enacted in 1995.[121]

---

[110] *Id.* at art. 8.2.

[111] *Id.*

[112] *Id.*

[113] *Id.* at art. 8.3.

[114] Commission Regulation 45/2001, 2000 O.J. (L 8) (EC)

[115] *See supra* note 97.

[116] *Id.*

[117] TFEU art. 16.1.

[118] TFEU art. 16.1.

[119] DPD, *supra* note 10, § 3.1.

[120] *Id.* at arts. 1.1.-2.

The Directive defines "personal data" as "any information relating to an identified or identifiable natural person."[122] The "processing of personal data" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[123] Finally, the Directive defines "data subject's consent" as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[124]

The Directive prescribes when the national laws of a Member State apply. According to the Directive, the national laws of a Member State apply to "processing of personal data" when:

> [T]he processing is carried out in *the context of the activities of an establishment* of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.[125]

The two part inquiry one must undertake to determine whether a Member State's national laws apply is, then, (1) does the data controller have an establishment located in said Member State and (2) does the data controller carry out the processing of personal data in the "context of the activities" of that establishment?[126]

As further clarified by the Article 29 Data Protection Working Party,[127] it is, thus, the "context of activities" and not the data's location that determines which national law is

---

[121] *Id.*

[122] *Id.* at art. 2(a).

[123] *Id.* at art. 2(b).

[124] *Id.* at art. 2(h).

[125] *Id.* at art. 4(1)(a) (emphasis added).

[126] *Id. See also*, W. Kuan Hon, et. al, *supra* note 104.

[127] *See infra* notes 141–143 and accompanying text for a discussion of the Art. 29 Data Protection Working Party.

applicable.[128] One must look to whether "an *establishment* of the controller is involved in *activities* relating to data processing."[129] The "degree of involvement" of the establishment in the data processing is a key factor.[130]

The Directive instructs Member States to condition the lawful processing of data in their respective jurisdictions on at least one of the following six clauses: (1) the data subject has given unambiguous consent;[131] (2) processing is necessary for implementation of a contract of the data subject or for fulfillment of the data subject's request prior to entry of a contract;[132] (3) processing is necessary for the data controller's legal compliance;[133] (4) processing is necessary for the protection of the data subject's vital interests;[134] (5) processing is necessary for the public interest or the "exercise of official authority vested in the controller or in a third party to whom the data are disclosed";[135] or (6) processing is necessary for pursuit of "legitimate interests" by the controller or a "third party to whom the data are disposed," except when in conflict with the data subject's "fundamental rights and freedoms" protected under Article 1.1 of the DPD.[136] The Directive requires that each Member State set up an independent supervisory authority to monitor data protection compliance in that state.[137]

With regard to consent, the Directive merely requires that it be "unambiguous," which allows for implied consent or consent by default.[138] This is in stark contrast to the BDSG, which requires express consent from an individual informed as to the purpose of the collection, processing, or use of personal data.[139] However, like the BDSG, the Directive

---

[128] *Opinion of The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data*, 2010 O.J. (L 281) at Part III, § 1(b).

[129] *Id*. (emphasis in original).

[130] *Id*.

[131] DPD, *supra* note 10, at art. 7(a).

[132] *Id.* at art. 7(b).

[133] *Id.* at art. 7(c).

[134] *Id.* at art. 7(d).

[135] *Id.* at art. 7(e).

[136] *Id.* at arts. 1.1 & 7(f). Article 1.1 of the DPD refers to the "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." *Id.* at art. 1.1.

[137] *Id.* at art. 28.1.

[138] *Id.* at art. 7(a).

[139] BDSG, *supra* note 2, §§ 4.1 & 4(a).1.

requires express consent for the collection of special types of data such as ethnicity, political affiliations, religion, or sexual orientation.[140]

4. Article 29 Data Protection Working Party

The Article 29 Data Protection Working Party (the "Article 29 Working Party" or "Working Party") is an advisory body to the Commission.[141] Article 29 of the Data Protection Directive created a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" to advise on data protection and privacy as an independent body.[142] The Working Party is comprised of representatives from each Member State, the EDPS, and the EU Commission.[143]

The Working Party is tasked with, *inter alia*, analyzing questions concerning the application of national laws that implement the Data Protection Directive, with an eye toward enhancing harmonization.[144] Notably, advising the EU Commission on proposed amendments of the DPD, such as the draft Data Protection Regulation, also falls within the scope of the Working Party's authority.[145] In fact, the Working Party first responded to the EU Commission's 25 January 2012 draft Regulation on 23 March 2012 and has continued to participate in the ongoing discussions.[146]

5. E-Privacy Directive

The European Parliament and Council Directive 2002/58 on Privacy and Electronic Communications, better known as the E-Privacy Directive, addresses data protection

[140] DPD, *supra* note 10, arts. 8.1–2(a). *See also*, BDSG, *supra* note 2, § 3.9.

[141] DPD, *supra* note 10, at art. 29.

[142] *Id.* at art. 29.1.

[143] *Id.* at art. 29.2; *see also*, *Member of the Article 29 Working Party*, EUROPEAN COMMISSION: JUSTICE, June 2, 2014, http://ec.europa.eu/justice/data-protection/article-29/structure/members/index_en.htm#h2-7 (last visited Feb. 22, 2014).

[144] Article 30 states, "The Working party shall . . . examine any question covering the application of the national measures adopted under [the Data Protection Directive] in order to contribute to the uniform application of such measures." DPD, *supra* note 10, at art. 30.1(a).

[145] *Id.* at art. 30.1(c).

[146] ART. 29 DATA PROTECTION WORKING PARTY, *Opinion 01/2012 on the Data Protection Reform Proposals*, 00530/12/EN, WP 191 (Mar. 23, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf; *see also, e.g.*, Art. 29 Data Protection Working Party, *Opinion 08/2012 Providing Further Input on the Data Protection Reform Discussions*, 01574/12/EN, WP199 (Oct. 5, 2012).

concerns in the communications sector.[147] The E-Privacy Directive was enacted in 2002 as a continuation of the DPD[148] and was revised in 2009.[149]

Of note is the E-Privacy Directive's notice of breach requirement, a provision that currently is not included in the DPD and, therefore, is not applicable to data breaches in other sectors.[150] The E-Privacy Directive, as amended, defines "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community." [151] The notice of breach provision states that:

> In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.[152]

The current draft of the new Data Protection Regulation includes a similar notice of breach provision based on the E-Privacy Directive.[153]

In relation to choice of law, the E-Privacy Directive defines what constitutes *establishment* of a company within a Member State.[154] The directive states that an "established services provider" is "a service provider who *effectively pursues an economic activity* using a fixed establishment for an indefinite period. The presence and use of the technical means and

---

[147] Council Directive 2002/58, 2002 O.J. (L 201), art. 1.1 (EC) [hereinafter "E-Privacy Directive"], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

[148] *Id*. at art. 4.2.

[149] Council Directive 2009/136, 2009 O.J. (L 337/11) (EC) (amending Council Directive 2002/22, 2002 O.J. (L 108) (EC), E-Privacy Directive, *supra* note 147, and Council Regulation No. 2006/2004, 2009 O.J. (L 337/11) (EC)) [hereinafter "Amendment to E-Privacy Directive"], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[150] Amendment to E-Privacy Directive, *supra* note 149, at art. 4.3.

[151] Amendment to E-Privacy Directive, *supra* note 149, at art. 2(c).

[152] Amendment to E-Privacy Directive, *supra* note 149, at art. 4.3.

[153] Data Protection Regulation, *supra* note 9, at art. 31-32.

[154] E-Privacy Directive, *supra* note 147, at art. 2(c).

technologies required to provide the service do not, in themselves, constitute an establishment of the provider."[155] The pursuit of economic activity factors heavily in the determination of where a company is established. According to the E-Privacy Directive,

> [T]he concept of establishment involves the *actual pursuit of an economic activity* through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but *the place where it pursues its economic activity*; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; *in cases where it is difficult to determine from which of several places of establishment* a given service is provided, *this is the place where the provider has the centre of his activities relating to this particular service*.[156]

Where the place of establishment is unclear because the company operates in multiple Member States, the law looks to the company's center of activity.[157]

The E-Privacy Directive anticipated that the law could be easily circumvented if tech companies chose to establish themselves in other Member States with more lenient standards.[158] In an effort to address and counter-act forum shopping, the E-Privacy Directive notes that the European Court of Justice (ECJ) "has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State" where the service provider's "choice of establishment was made with a view to evading the legislation that would have applied to the provider had he

[155] E-Privacy Directive, *supra* note 147, at art. 2(c) (emphasis added).

[156] Council Directive 09/31, art. 19, 2000 O.J. (L 178) (EC) (emphasis added).

[157] *Id.*

[158] *Id.* at recital 57.

been established on the territory of the first Member State."[159] Although the ECJ has affirmed that Member States may take measures to prevent forum shopping and evasion of national law,[160] the ECJ has also held that Member States must consider possible abuses on a case-by-case basis[161] and that an entity establishing itself in another Member State in which it conducts no business "is not sufficient to prove the existence of abuse or fraudulent conduct . . . ."[162] Moreover, according to the ECJ, where an entity chooses to establish itself "in the Member State whose rules of company law seem to him the least restrictive and to set up branches in other Member States cannot, in itself, constitute an abuse of the right of establishment."[163] At odds with the EU's goal of creating a Single Market, a Member State's ability to pursue and prevent forum shopping is limited by EU policies such as the Freedom of Establishment[164] and the Free Movement of Goods.[165]

C. Recent Cases and Key Issues

I. Applicability of National Law—Facebook "Real Names" Policy & Apple Privacy Policy

1. Facebook "Real Names" Policy

Under the German Telemedia law—the TMG—consumers of online services are entitled to anonymous or pseudonymous use of those services.[166] This means that German individuals should have the right to operate under pseudonyms when using social media websites such as Facebook.[167] However, in a recent high profile challenge brought by German data

[159] *Id*. *See also*, D.H.M. Segers v. Bestuur van de Bedrijfsvereniging voor Bank- en Verzekeringswezen, Groothandel en Vrije Beroepen, CJEU Case C-79/85, 1986 E.C.R I-2375; Centros Ltd v. Erhvervs- og Selskabsstyrelsen, CJEU Case C-212/97, 1999 ECR I-1459.

[160] *Centros*, CJEU Case C-212/97 at para. 24.

[161] *Id*. at para. 25.

[162] *Id*. at para. 29. *See also*, *D.H.M. Segers*, CJEU Case C-79/85 at para. 16; Tom O'Shea, *Tax Avoidance and Abuse of EU Law*, 11 EC TAX J. 77 (2010), http://www.ccls.qmul.ac.uk/docs/staff/oshea/52174.pdf.

[163] *Centros*, CJEU Case C-212/97 at para. 27.

[164] TFEU, *supra* note 95, at art. 49 (stating that "restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State shall be prohibited").

[165] TFEU, *supra* note 95, at art. 34–36.

[166] TMG, *supra* note 3, § 13.6.

[167] Press Release, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) [Independent State Center for Data Protection Schleswig-Holstein], *ULD Issues Orders Against Facebook Because of Mandatory Real Names* (Dec. 17, 2012), https://www.datenschutzzentrum.de/presse/20121217-facebook-real-names.htm.

protection authorities against Facebook's "Real Names Policy," a German administrative court decided this is not the case.[168]

Facebook's Real Names Policy requires users to register for accounts using their real names and bans the use of fake names or nicknames.[169] This policy clearly is at odds with the provisions of the TMG.[170] The *Unabhängigen Landeszentrums für Datenschutz* (ULD) (Independent Center for Data Protection), a German data protection authority, took action against Facebook after the social media giant refused to change its policy.[171] On 17 December 2012 the ULD issued a ruling barring Facebook's Real Names Policy.[172] Facebook appealed the order and on 14 February 2013 the presiding Schleswig-Holstein Administrative Court ruled in Facebook's favor on the grounds that Facebook is not subject to German data protection law.[173] The court's reasoning was based on the BDSG and EU Data Protection Directive provisions exempting data controllers that are established in another Member State and do not carry out data processing through a branch in Germany from German law.[174] As Facebook is headquartered in Ireland and its German branch only performs marketing and advertising functions unrelated to data processing, the court found that Facebook is subject to Irish, not German, law.[175] Ireland guarantees no explicit right to the anonymous use of online services.[176] ULD appealed the decision, but the Schleswig-Holstein Administrative Court of Appeals upheld the lower court's decision in Facebook's favor.[177]

---

[168] *See* Press Release, ULD, *supra* note 5.

[169] *Id.*

[170] TMG, *supra* note 3, § 13.6 (guaranteeing an individual's right to anonymous or pseudonymous use of telemedia services).

[171] *See* Press Release, ULD, *supra* note 5.

[172] *Id.*

[173] Verwaltungsgericht [VG - Administrative Court], Case No. 8 B 60/12 (Feb. 14, 2013) (Ger.), https://www.datenschutzzentrum.de/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf; *see also*, Schleswig-Holstein Administrative Court, *Verwaltungsgericht gibt Eilanträgen von Facebook statt* [Administrative Court Grants Facebook's Application for Interim Relief], Feb. 15, 2013, http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/15022013VG_facebook_anonym.html.

[174] *Supra* note 173, *See also*, BDSG, *supra* note 2, § 5; DPD, *supra* note 10, at art. 4(1)(a).

[175] *Id.*

[176] The Irish Data Protection Commissioner audited Facebook Ireland Ltd. in December 2011 and published a review of Facebook's implementation of the audit recommendations the following year, reporting that Facebook had "advanced sufficient justification for child protection and other reasons for their policy of refusing pseudonymous access to its services." IRISH DATA PROTECTION COMMISSIONER, *Facebook Ireland Ltd: Report of Re-Audit* 11, 50–51 (Sept. 21 2012), http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.

[177] *See* Press Release, ULD, *supra* note 5.

This case illustrates that the methods adopted by both Germany and the EU for determining applicability of national law (using country of origin principles[178]—which focus on the geographical location of data processing and use—instead of marketplace principles[179]—which look toward the point of sale), make it particularly easy for technology and internet based companies to circumvent German data protection law.

2. Apple Privacy Policy

In contrast, a Berlin regional court recently applied German data protection laws to Apple when striking down several clauses of Apple's privacy policy.[180] The case "is important because the court interpreted the relevant data protection clauses in accordance with German data protection law rather than Irish data protection law."[181] Apple, like Facebook, has situated its European headquarters in Ireland.

The German consumer watchdog *Verbraucherzentrale Bundesverband* (VZBV) (Federation of German Consumer Organizations) challenged fifteen clauses in Apple's privacy policy; Apple voluntarily withdrew seven of those clauses, leaving eight up for consideration by the court.[182] On 30 April 2013, the *Landgericht Berlin* (District Court) ruled that the remaining eight clauses in Apple's privacy policy violated the BDSG, UWG, TMG, and TKG (Telecommunications Act) as well as the German civil code.[183] For example, the court found the global consent required by Apple's privacy policy to be invalid because

[178] Council Directive 2000/31, 2000 O.J. (L 178), at recital 22 (EC).

[179] The draft Data Protection Regulation utilizes the marketplace principle with regard to third parties located outside the EU, but doing business within or directing services toward the EU: "Those who intend to do business in Europe and want to collect personal data in this context should also be subject to European data protection law when servers and corporate headquarters are located outside the EU (marketplace principle)." Peter Schaar, *EU Data Protection Package: A Real Chance for Better Data Protection!*, THE FED. COMMISSIONER FOR DATA PROTECTION & FREEDOM OF INFO., Mar. 19, 2012, http://www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/blog/EUDataprotectionPackage.html?nn=1269676.

[180] Landgericht [LG - District Court], Case No. 15 O 92/12 (Apr. 30, 2013), http://www.vzbv.de/cps/rde/xbcr/vzbv/Urteil_des_LG_Berlin_zur_Datenschutzrichtlinie_von_Apple.pdf.

[181] HUNTON & WILLIAMS LLP, *German Court Rules Apple's Privacy Policy Violates German Law*, May 8, 2013, http://www.huntonprivacyblog.com/2013/05/articles/german-court-rules-apples-privacy-policy-violates-german-law/.

[182] *Datenklauseln von Apple rechtswidrig* [Data Clauses of Apple Illegal], THE CONSUMER FEDERATION (VZBZ), May 7, 2013, http://www.vzbv.de/11558.htm.

[183] 15 O 92/12 (Ger.).

consumers were not sufficiently informed as to how their personal data would be used and exactly with whom Apple would share the data.[184]

The court also objected to a clause stating Apple's intent to use consumers' location or GPS data in order to offer these consumers' location-based services and products.[185] Apple's privacy policy claimed that any data collected by Apple regarding the location of a consumer's Apple device would be anonymous.[186] The court found that the data would not be anonymous because it is not possible to offer location-based services and products without some connection of the data with an individual's attributes.[187] Because Apple's European headquarters are in Ireland, if Apple were to appeal the Berlin regional court's decision, it is unclear whether the appeals court would find that Apple is subject to German law or, like Facebook, only to Irish data protection law.

II. Lack of Accountability—Google Profile Building & Amazon Returns Policy

1. Google Profile Building

In March 2012, Google unveiled a new privacy policy, much to the chagrin of EU and Member State regulators.[188] The new privacy policy would allow Google to create a *master profile* for a user comprised of information tracked across multiple sites, such as Google search, Gmail, and YouTube, for the purposes of targeted advertising.[189]

Regulators took issue with the policy change's notice—claiming it did not accurately inform users as to how their data would be tracked across websites or the intended use of that data once collected—and the fact that if users withheld their consent to the new privacy policy, they would be barred from further access to Google's services.[190] This meant that users had no practical way to decline Google's proposed tracking; ceasing use of Google's

---

[184] Loek Essers, *Apple's Privacy Policy Violates German Data Protection Law,* Computerworld, May 7, 2013, http://www.computerworld.com/s/article/9238978/Apple_39_s_privacy_policy_violates_German_data_protection_law_Berlin_court_rules.

[185] 15 O 92/12 (Ger.).

[186] Essers, s*upra* note 184.

[187] *See* 15 O 92/12 (Ger.).

[188] Christopher Williams, *Google Could Face EU "Repressive Action" on Privacy*, THE TELEGRAPH, Feb. 18, 2013, http://www.telegraph.co.uk/technology/google/9877694/Google-could-face-EU-repressive-action-on-privacy.html.

[189] *Id.*

[190] *Id.* Conditioning use of online services on consent runs afoul of TMG, *supra* note 3, § 12.3.

services was the only recourse and, for Gmail account holders, for example, not realistic.[191] The EU demanded that Google withdraw the policy change and gave Google four months to respond before the EU would initiate legal proceedings.[192] Google failed to respond.[193]

Google continues to insist publicly that its new privacy policy complies with EU data protection laws.[194] Faced with Google's unwillingness to withdraw the policy change, several Member States, including Germany, announced coinciding investigations into whether the policy is in compliance with data protection laws at the national level.[195] As part of this concerted effort, the *Hamburgisch Beauftragte für Datenschutz und Informationsfreiheit* (Hamburg Commissioner for Data Protection and Freedom of Information) filed a complaint in July 2013 against Google that has yet to be resolved.[196] In a separate action, the same Berlin regional court that ruled against Apple's privacy policy earlier in the year found on 19 November 2013 that Google's new privacy policy likewise violated the BDSG.[197] The German consumer watchdog VZBV had filed a complaint against Google in July 2012, a few months after Google unveiled the controversial policy change.[198] The Berlin regional court held that twenty-five of Google's privacy policy and terms of service clauses were too vague.[199] Google's European headquarters are in Ireland, like Facebook and Apple, though "most of its European revenues are generated outside Ireland—from the UK and . . . Germany."[200]

---

[191] Williams, *supra* note 188.

[192] *Id.*

[193] *Id.*

[194] Eric Pfanner, *Google Faces More Inquiries in Europe over Privacy Policy*, N.Y. TIMES, Apr. 2, 2013, http://www.nytimes.com/2013/04/03/technology/google-to-face-national-regulators-over-privacy-policy.html?_r=0.

[195] Williams, *supra* note 188.

[196] Loek Essers, *Berlin Court Rules Google Privacy Policy Violates Data Protection Law*, PCWORLD, Nov. 20, 2013, http://www.pcworld.com/article/2065320/berlin-court-rules-google-privacy-policy-violates-data-protection-law.html.

[197] Landgericht [LG - District Court], Case No. 15 O 402/12 (Nov. 19, 2013), http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20131217.1510.392784.html (Ger.).

[198] David Meyer, *German Court Chides Google over Its Vague Privacy Policy and Terms*, GIGAOM, Nov. 20, 2013, http://gigaom.com/2013/11/20/german-court-chides-google-over-its-vague-privacy-policy/.

[199] Jabeen Bhatti, *Berlin Court Rules Google Privacy Policy Too Vague; Internet Giant Set to Appeal*, BLOOMBERG BNA, Nov. 25, 2013, http://www.bna.com/berlin-court-rules-n17179880340/.

[200] Lisa O'Carroll, *If Google Is in Ireland for Tax Reasons, Why Are Most of Its Profits in Bermuda?*, THE GUARDIAN, Mar. 24, 2011, http://www.guardian.co.uk/business/ireland-business-blog-with-lisa-ocarroll/2011/mar/24/google-ireland-tax-reasons-bermuda.

In an unrelated case, the Hamburg Commissioner for Data Protection and Freedom of Information fined Google €145,000 in April 2013 for data privacy breaches associated with Google Street View.[201] The breach stemmed from Google's unwitting and illegal collection of unsecured data from individuals' Internet routers as Google's car fleet of rolling cameras filmed pictures for its Street View service.[202] This case is distinguished from the Facebook case (as noted above) because Google's collection of data for its Street View service took place in Germany.[203] Google expressed regret for the breach and agreed to pay the fine,[204] which, however, was an insignificant amount compared to Google's annual revenue.[205]

2. Amazon Returns Policy

In 2010, a number of consumers in the United Kingdom (UK) who had purchased products from Amazon UK lodged complaints regarding Amazon's returns policy.[206] These consumers soon learned that Amazon was not subject to the consumer laws of the UK, but to those of Luxembourg, the site of Amazon's European headquarters.[207] As a result, Amazon was also subject to EU consumer law.[208] Under EU law, consumers are entitled to a two-year manufacturer warranty on all products.[209] Because the UK only partially adopted these provisions, the status of warranty rights in the UK was unclear,[210] so Amazon being held to a two-year manufacturer warranty was viewed as a positive

---

[201] Ian Steadman, *Google Fined by German Regulator over Street View Privacy Breach*, WIRED, Apr. 22, 2013, http://www.wired.co.uk/news/archive/2013-04/22/google-germany-fine.

[202] *Id.*

[203] Friedrich Geiger, *German City of Hamburg Fines Google over Street View Service*, WALL ST. J. ONLINE, Apr. 22, 2013, http://online.wsj.com/article/SB10001424127887324874204578438714112912742.html# (noting the Hamburg Commissioner for Data Protection "ordered [Google] to pay 145,000 euros ($189,000) for collecting data of private Wi-Fi networks when Google's cars drove through the streets [of Hamburg] to take pictures from 2008 until 2010").

[204] Steadman, *supra* note 201.

[205] The fine "represents about 0.002 percent of [Google's] total net profit in 2012." Zack Whittaker, *Germany Fines Google for "Unprecedented" Street View Wi-Fi Data Breach*, ZDNET, Apr. 22, 2013, http://www.zdnet.com/germany-fines-google-for-unprecedented-street-view-wi-fi-data-breach-7000014337/.

[206] Miles Brignall, *Amazon's Luxembourg Base Means Improved Consumer Rights*, THE GUARDIAN, Apr. 30, 2010, http://www.guardian.co.uk/money/2010/may/01/amazon-luxembourg-improved-consumer-rights.

[207] *Id.*

[208] *Id.*

[209] Council Directive 99/44, 1999 O.J. (L 171/12), at art. 5.1 (EC).

[210] *Two-Year Warranty (EU Law)*, THIS IS MONEY, Jan. 26, 2010, http://www.thisismoney.co.uk/money/bills/article-1677034/Two-year-warranty-EU-law.html.

outcome for UK consumers.[211] The fact that Amazon was under Luxembourg's jurisdiction, however, presented enforcement challenges to UK consumers who received unsatisfactory responses from Amazon and believed Amazon's practices were not in line with EU law.[212]

For instance, some consumers who sought a repair or replacement of a product within two years of purchase faced resistance from Amazon.[213] The UK European Consumer Centre,[214] which is responsible for cross-border complaints arising in the UK, sent a file of complaints from UK consumers to authorities in Luxembourg.[215] Luxembourg met with Amazon and instructed the company to "make consumer rights more transparent on its website" and to respond to the UK complaints.[216] Although the UK European Consumer Centre was able to help facilitate communication, it had no authority over Amazon.[217] According to the UK European Consumer Centre, a UK consumer wishing to pursue a refund from Amazon must "file a small claim in the UK, which will then be forwarded to be heard in the relevant EU jurisdiction, in this case Luxembourg."[218] Thus, Luxembourg authorities determined how and to what extent the EU consumer law was enforced against Amazon.

D. Draft European Union Data Protection Regulation

Following an evaluation of the effectiveness of the EU data protection framework, the Commission reported in 2010 that "the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection."[219] On 25 January 2012, the European Commission issued the draft Data Protection Regulation.[220] With promulgation

---

[211] *See* Brignall, *supra* note 206.

[212] *Id.*

[213] *Id.*

[214] According to the UK European Consumer Centre's website, "[t]he network of European Consumer Centres (ECC-Net) serves EU consumers shopping for goods and services on the European market, providing them with advice on their EU consumer rights and helping them with their disputes with traders in other EU countries." UK EUROPEAN CONSUMER CENTRE, http://www.ukecc.net/about/index.cfm.

[215] *See* Brignall, *supra* note 206.

[216] *Id.*

[217] *Id.*

[218] *Id.*

[219] Data Protection Regulation, *supra* note 9, at 2 (referencing *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*, COM (2010) 609 Final (Nov. 4, 2010)).

[220] *Id.*

of the Data Protection Regulation, the EU aims to harmonize data protection law across Member States, thereby securing individuals' rights to data protection and, at the same time, furthering development of the Single Market.[221] The Regulation seeks to bring EU data protection law up to date with current technology[222] and will supersede the Data Protection Directive and Member States' national data protection laws, including the BDSG, when it comes into force in 2015 or 2016.[223]

I. Current Provisions

The current negotiations regarding amendments to the draft of the Data Protection Regulation revolve around several key issues, such as, the right to be forgotten, explicit consent, the right to object, profiling, and leveling disparities among Member State's laws.[224]

1. Right to be Forgotten

The draft Data Protection Regulation provides for a "right to be forgotten and to erasure."[225] Under Article 17, data subjects may require data controllers to delete their personal data and refrain from further dissemination of that data.[226] Exceptions to this right include data retention that is necessary for freedom of expression,[227] public interest in relation to public health,[228] research of a historical, statistical, or scientific nature,[229] and compliance with legal obligations.[230]

---

[221] *Id.*

[222] *Id.* § 2 of the Explanatory Memorandum.

[223] *Id.* §§ 3.1–.2 of the Explanatory Memorandum. Once the Regulation is passed by the EU, Member States will have an additional two years to bring national laws into line with the Regulation. *Id.* at art. 91.

[224] Examples of other issues currently in negotiation are data portability, the use of plain language by data controllers, penalties for noncompliance, and appointment of a data protection officer at companies over a certain size. *Q&A on EU Data Protection Reform*, EUROPEAN PARLIAMENT (Oct. 22, 2013, 10:13 AM), http://www.europarl.europa.eu/news/en/pressroom/content/20130502BKG07917/html/QA-on-EU-data-protection-reform.

[225] Data Protection Regulation, *supra* note 9, at art. 17.

[226] *See id.* at art. 17.1.

[227] *See id.* at art. 17.3(a).

[228] *See id.* at art. 17.3(b).

[229] *See id.* at art. 17.3(c).

[230] *See id.* at art. 17.3(d).

2. Explicit Consent

Processing of personal data is conditioned upon explicit consent in the draft Data Protection Regulation.[231] The Regulation defines "data subject's consent" as "any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed."[232]

The Data Protection Regulation further clarifies that the data subjects have the right to withdraw consent at any time.[233] Addressing prominent data controllers such as Google, the Regulation states that consent may not serve as legitimate grounds for data processing "where there is a significant imbalance between the position of the data subject and the controller."[234]

3. Right to Object and Profiling

Under Article 19, data subjects have the right to object to processing of personal data for the purposes of direct marketing.[235] The data controller must explicitly and clearly offer the opportunity to object.[236]

Under Article 20, the Data Protection Regulation limits the instances in which data controllers may create profiles based on personal data.[237] Data subjects generally have a right to be free from profiling.[238] However, the Regulation does allow profiling that is (1) necessary for the entry into or completion of a contract;[239] (2) expressly authorized by EU or a Member State's law;[240] or (3) consented to by the data subject.[241]

---

[231] *See id.* at art. 4.8 & 7.

[232] *See id.* at art. 4.8.

[233] *See id.* at art. 7.3.

[234] *See id.* at art. 7.4.

[235] *See id.* at art. 19.2.

[236] *Id.*

[237] *See id.* at art. 20.1.

[238] *Id.*

[239] *See id.* at art. 20.2(a).

[240] *See id.* at art. 20.2(b).

[241] *See id.* at art. 20.2(c).

4. Consistency Mechanism

In an effort to level the playing field amongst Member States, the Data Protection Regulation "introduces a consistency mechanism for ensuring unity of application in relation to processing operations which may concern data subjects in several Member States."[242] Under Article 57, the Regulation requires the data protection supervisory authorities in each Member State to co-operate with each other and the Commission.[243] The European Data Protection Board (EDPB) (the new EU supervisory body that will replace the Article 29 Working Party)[244] or any Member State's supervisory authority may request use of the consistency mechanism; the consistency mechanism involves review of proposed measures related to data processing, with the goal of ensuring "correct and consistent application" of the Data Protection Regulation.[245] Once the consistency mechanism is engaged, the EDPB will issue an opinion on the case at hand.[246] The Commission also may issue an opinion.[247] The Member State supervisory authority that has proposed the measure in dispute will then take both opinions into account and relay to the EDPB and the Commission whether it will follow the recommended course of action and, if not, its justification for the departure.[248] If the Member State supervisory authority intends not to follow the opinions, the Commission may issue a binding decision suspending the Member State's proposed measure.[249]

Additionally, the Member State in which a data controller is headquartered will determine which state supervisory authority has jurisdiction.[250] Like the DPD, the Regulation applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union."[251] The Regulation goes further, however, by extending its scope to data controllers or processors outside the EU so long as they are

[242] *See id.* § 3.4.7.2 of the Explanatory Memorandum.

[243] *Id.* at art. 57.

[244] *See id.* at art. 64.

[245] *See id.* at arts. 58.3–.4.

[246] *See id.* at art. 58.7.

[247] *See id.* at art. 59.1.

[248] *See id.* at arts. 58.8, 59.2, 59.4.

[249] *See id.* at art. 60.

[250] *See id.* at arts. 3.1, 4.13.

[251] *See id.* at art. 3.1; *see also*, DPD, *supra* note 10, at art. 4(1)(a).

"offering . . . goods or services to . . . data subjects in the Union . . . or . . . monitoring . . . their behaviour."[252]

II. The Way Forward

Almost 4,000 amendments have been taken under consideration since the Commission released the draft Data Protection Regulation.[253] Which of these proposed amendments ultimately are adopted remains to be seen.[254] Both the EU Parliament and the Council must approve the Regulation before it can become law.[255] The goal is to pass the legislation before EU elections in May 2014.[256]

The Civil Liberties, Justice and Home Affairs Committee (LIBE), the EU Parliament's lead committee on the Regulation, was originally scheduled to vote on the proposed amendments on 29 May 2013, but the vote was postponed and did not take place until 21 October 2013; in the vote, LIBE approved all of the 104 compromise amendments presented by rapporteurs Jan-Philipp Albrecht and Dimitrios Droutsas.[257] In a *trilogue* meeting that is to take place after the LIBE vote, the EU Commission, Council, and Parliament will agree to and decide on the text of the Regulation.[258] Following the trilogue, the Parliament will need to vote in plenary to adopt the Regulation.[259] With the delayed

[252] Data Protection Regulation, *supra* note 9, at art. 3.2.

[253] See supra note 224. Several groups have proposed amendments, including MEP Jan Philipp Albrecht, the LIBE rapporteur, on behalf of the Parliament, and Germany. Data Protection Regulation, *supra* note 9, at art. 3.2. *See also*, Press Release, German Minister for the Interior Hans-Peter Friedrich and EU Justice Commissioner Viviane Reding Emphasise the Importance of the EU General Data Protection Regulation for the Digital Single Market and the Protection of Fundamental Rights in Europe (Mar. 7, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-177_en.htm?locale=en.

[254] *See* Press Release, German Minister for the Interior Hans-Peter Friedrich and EU Justice Commissioner Viviane Reding Emphasise the Importance of the EU General Data Protection Regulation for the Digital Single Market and the Protection of Fundamental Rights in Europe (Mar. 7, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-177_en.htm?locale=en..

[255] Simon Elliott, *The EU Date Protection Regulation: Timing*, PRIVACY & DATA SEC. BLOG, Feb. 27, 2013, http://www.privacydatasecurityblog.com/2013/02/27/the-data-protection-regulation-where-are-we/.

[256] *See supra* note 224.

[257] John O'Connor, *EU Data Protection Vote Delayed*, LEXOLOGY, May 8, 2013, http://www.lexology.com/library/detail.aspx?g=781c955a-3fbf-40ba-967a-14cbaf7dfb35; *see also* Press Release, Libe Committee Vote Backs New EU Data Protection Rules (Oct. 22, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[258] *See* Elliott, *supra* note 255.

[259] *Id.*

LIBE vote, EU regulators have called for the various parties to focus on readily coming to an agreement in order for the plenary vote to take place before the 2014 elections.[260]

Considering the present legal inequities within the EU, Germany should make an all-out effort in the ongoing negotiations to ensure that the final version of the Data Protection Regulation curtails current and prevents future forum shopping and upholds fair competition across Member States. To do this, there are several approaches the German government could champion regarding amendment of the Regulation.

For one, choosing to base the application of national law on the marketplace as opposed to the country of origin (expressed as the data controller's place of processing or "context of the activities" in the DPD and as its European headquarters in the current iteration of the Data Protection Regulation) would go a long way toward curbing forum shopping.[261] It would help to correct cases like Google, which chose to locate its headquarters in Ireland, but profits significantly from German consumers.[262] Additionally, one could argue that this would make the draft Regulation more consistent, as the draft Regulation already utilizes the marketplace principle with regard to third parties outside the EU.[263]

Another possible equalizer would be to require the same level of consent in the Data Protection Regulation as is currently required in the BDSG. Under the draft Regulation, implied consent or consent by default are no longer allowed; instead, the draft Regulation requires "explicit consent."[264] In comparison, the BDSG requires express consent from an individual informed as to the purpose of the collection, processing, or use of personal data.[265] The closer the Regulation comes to the BDSG, the more likely the standards in other Member States will match those in Germany.

As discussed, the Data Protection Regulation is taking a page from the E-Privacy Directive by incorporating a similar notice of breach requirement.[266] Likewise, the EU should consider incorporating the E-Privacy Directive's provision on forum shopping into the

---

[260] *Id.*; *see also*, Allison Grande, *EU Regulators Urge Swift Action on Data Protection Reform*, LAW360, Dec. 4, 2013, http://www.law360.com/articles/493310/eu-regulators-urge-swift-action-on-data-protection-reform.

[261] *See supra* notes 179180 and accompanying text.

[262] *See* O'Carroll, *supra* note 200.

[263] *See supra* notes 253254 and accompanying text.

[264] Data Protection Regulation, *supra* note 9, at arts. 4.8 & 7.

[265] BDSG, *supra* note 2, §§ 4.1 & 4(a).1.

[266] *Compare* Data Protection Regulation, *supra* note 9, at arts. 31 & 32, *with* Amendment to E-Privacy Directive, *supra* note 147, at art. 4.3.

Regulation.[267] The provision acknowledges that companies may seek to evade legislation in Member States with higher standards and notes that the European Court of Justice has confirmed Member States are entitled to take measures against those companies that engage in forum shopping.[268] Because the ECJ has significantly limited that right, however, the Regulation must go further and identify situations in which a Member State's right to address forum shopping supersedes other EU guarantees.[269]

Finally, ensuring that the EU has a robust and active enforcement mechanism will be imperative to the Regulation's ability to level disparities among data protection standards of Member States.[270] This will depend partly on whether the enforcement—or, as in the draft Regulation, the consistency—mechanism is sufficiently funded.[271] Germany should also encourage the EU to use this enforcement authority through either the EDPB or the Commission without hesitation and for high profile cases, immediately and publicly, for any Member State supervisory authorities that choose not to follow EDPB or Commission opinions.[272] The Commission must be ready to exercise its authority, which is discretionary under the current draft,[273] so that the authority does not just theoretically exist, but tangibly and powerfully sets an early example. Germany should push to ensure that the EU enforcement mechanism is sufficiently funded and retains a binding authority, veto, or similar power.

E. Conclusion

The EU is in the process of creating a new set of laws in an attempt to create a more equal playing field. This is especially important for companies whose operations are based in Member States with higher regulation, like Germany, and face forum shopping by competitors. However, at this point in the legislative process, it is unclear what the final version of the new Data Protection Regulation will look like and, therefore, how the Regulation will be applied and enforced. If EU regulators choose to take a reserved approach and to allow Member States wide latitude in enforcing the Regulation, companies can expect little to change. Therefore, for German companies that comply with data protection laws and are in a Member State that will enforce the Regulation to its

[267] E-Privacy Directive, *supra* note 147, at Recital 57.

[268] *Id.*

[269] *See supra* notes 159164 and accompanying text.

[270] *See supra* Part C.II.

[271] *See* W. Kuan Hon, et. al, *supra* note 104.

[272] *See supra* notes 248251 and accompanying text.

[273] Data Protection Regulation, *supra* note 9, at art. 60.

fullest extent the most important factor could be German government, industry, and consumers working hard to encourage EU regulators to take a strong stand in ensuring the new data protection measures will be applied and enforced consistently across all Member States. Otherwise, companies that play by the rules and Member States that enforce those rules will continue losing out to the laxer members of the EU, and all EU Member States, not to mention their consumers, will suffer from the lack of a true Single Market.

As noted earlier, the new Data Protection Regulation is not estimated to come into effect until 2015 at the earliest.[274] In the meantime, it would be tempting for German companies enduring an unequal playing field to lobby and encourage the German government to engage with Member States like Ireland or Luxembourg in a race to the bottom in terms of data protection standards. But, understanding the historical significance[275] and place of prominence data protection enjoys in Germany, as well as the social awareness of German consumers, [276] this would likely be neither advisable nor in those companies' long term interests.

Instead, it would be better for those companies to spend time and energy—first—educating consumers and legislators as to the pitfalls of the current data protection regulatory scheme and the disadvantage that German companies face when their direct competitors are allowed to be less respectful of consumer data privacy through forum shopping and—second—working with German and EU legislators to effect amendments to the Data Protection Regulation, such as adopting marketplace principles and sufficient enforcement mechanisms, that will help the Regulation curtail forum shopping and ensure consistent application.

Companies facing an unequal playing field should help EU consumers, a disproportionate number of whom are German, understand that their data is not being treated with the same respect EU-wide and will not be in the future unless the Data Protection Regulation has stronger provisions mandating it.[277] For a German company, this might take the form of a German or even EU-wide advertising campaign both trumpeting the company's

[274] *See supra* Part D.

[275] *See* Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 GERMAN L.J. 291, 291 (2010) (noting the "evolving corpus of [data protection] law [in Germany] exhibits a singularly-German mindfulness of the historical significance of abrogating fundamental rights within constitutional democracy").

[276] In a Eurobarometer survey, 69% of Germans questioned think their "specific approval" should be sought before any collection and processing of personal data. *Attitudes on Data Protection and Electronic Identity in the European Union*, EUROPEAN COMMISSION: EUROBAROMETER 74.3, Jun. 2011, at 3, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_de_en.pdf. According to that same survey, only 34% of Germans trust online shops will protect their personal data. *Id*.

[277] Over 70% of Germans shop online. *Id.* at 1.

respect for consumers' data protection and warning against its competitors' practices of shopping for the processing location that allows for the least respect of consumers' private data.[278] Some means of creatively and cost-effectively promoting awareness on these issues include partnering with grassroots (and "netroots") pro-privacy organizations[279] to create online content and videos that can spread virally from friend to friend as well as using more traditional forms of media and lobbying.[280] Even if successful in educating the public and passing helpful amendments to the Data Protection Regulation, it will be equally important to ensure that the EU regulators tasked with overseeing the Regulation have the resources and funding to successfully audit and enforce consistent application. Only then will the forthcoming Data Protection Regulation provide real privacy protection and ensure a level playing field for compliant companies EU-wide.

[278] According to a Berlin study, German consumers will choose companies that offer more protection of their data privacy over companies that offer less protection when there is little or no price differential, but the discrepancy between the companies' privacy policies must be clear. DR. NICOLA JENTZSCH ET AL., STUDY ON MONETISING PRIVACY – AN ECONOMIC MODEL FOR PRICING PERSONAL INFORMATION (2012), *available at* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy ("If there are little to no differences in the prices offered by service providers on homogeneous goods, a competitor who has a reduced data requirement (privacy- friendly service provider) can obtain a competitive advantage as long as this type of differentiation is obvious to the consumer").

[279] For example, a successful movement to challenge the 2007 implementation of the EU Data Retention Directive in Germany "consisted of highly-networked civil and digital rights activists, ideologically-heterogeneous students and academics, and German or European NGOs." Desimone, *supra* note 275, at 306.

[280] The use of media helped raise awareness for the anti-EU Data Retention Directive movement: "The success of German groups in raising public awareness of a highly-technical topic, publicizing their rarely-at-odds messages, and organizing successful demonstrations and legal actions can be attributed to an extraordinarily effective use of new networked media to convey resources, ideas, and people around Germany and Europe." *Id.* at 307.