EUROPEAN ENFORCEMENT TARGETING U.S. TECH COMPANIES: GROWING CONNECTIONS BETWEEN DATA PROTECTION AND COMPETITION LAW

by

Carter Manny*

* Professor of Business Law, University of Southern Maine

EUROPEAN ENFORCEMENT TARGETING U.S. TECH COMPANIES: GROWING CONNECTIONS BETWEEN DATA PROTECTION AND COMPETITION LAW

Introduction

Large U.S. technology companies collect and analyze huge amounts of personal data from users all over the world. Use of that information raises concerns about privacy, especially in Europe under the strict provisions of the European Union's General Data Protection Regulation.[1] The largest U.S. tech businesses have been described as resembling nation-states because they control economic systems that are larger than most national economies.[2] Facebook, for example, has more than 1.5 billion users, a population larger than China's.[3] The size of the businesses, and their large market shares, also raise concerns about abuse of their dominant positions under European competition law, which is equivalent to U.S. antitrust law.[4] For many years, regulators have considered connections between legal principles in data protection and competition.[5] In early 2019, those connections were made in an enforcement action by the German Cartel Office in a case against Facebook. This paper seeks to provide context for the integrated approach by examining enforcement actions in Europe against U.S. tech companies, first under data protection law and then under competition law. Next, the history of the movement toward a combined approach is summarized. Implementation of the combined analysis is examined under the German case. Finally, the need to adapt traditional methodologies in enforcement actions is considered.

I. Data Protection Enforcement by European Data Protection Authorities

A. Enforcement in France

France has taken the lead in imposing massive fines on U.S. tech companies for violations of European privacy law. In January 2019 the French data protection authority fined Google €50 million for violating the GDPR by failing to provide adequate disclosure of information and for failing to obtain adequate consent from users.[6] The regulators found that information provided by the company was not easily accessible. Data processing purposes, storage periods and categories of data use for personalization of ads, were scattered across several pages and were accessible only

[1] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L119) 1 [hereinafter GDPR].
[2] See GEOFFREY G. PARKER, MARSHALL W. VAN ALSTYNE & SANGEET PAUL CHOUDARY, PLATFORM REVOLUTION 159 (2018).
[3] *Id.*
[4] Consolidated Version of the Treaty on the Functioning of the European Union art. 102., May 9, 2008, 2008 O.J. (C115) 89 [hereinafter TFEU].
[5] *See infra* Part III.
[6] *See, e.g.,* NATIONAL DATA PROTECTION COMMISSION, THE CNIL'S RESTRICTED COMMITTEE IMPOSES A FINANCIAL PENALTY OF 50 MILLION EUROS AGAINST GOOGLE LLC, https://www.dnil.fr/en/cnils-restricted-committee-imposes – financial-penalty-50-million-euros-against-google-llc (last visited Mar. 12, 2019)[hereinafter *CNIL Decision*].

by following five or more steps. Purposes of processing and categories of data were described vaguely. Retention periods for data were not always specified.[7]

Google stated that it relied on user consent to process data for the purpose of personalizing ads. However, the French data protection authority concluded that users' consent was not properly obtained for two reasons: consent was not sufficiently informed, and consent was neither "specific" nor "unambiguous" as required by data protection law.[8] Because information about processing operations for personalization of ads was scattered across several pages, users would have difficulty understanding the extent of their consent. Although it was possible for a user to modify some options of the account by clicking on a button labeled "more options," the step for the creation of the account sought generalized consent by requiring the user to tick two boxes: one titled "I agree to Google's Terms of Service" and another titled "I agree to the processing of my information as described above and further explained in the Privacy Policy." Google's terms therefore required the user to provide consent to all the processing operations, which violated the GDPR's provision that consent is "specific" only if it is given distinctly for each purpose.[9] In addition, after clicking on the "more options" button, the user was presented with an advertising personalization page with pre-ticked boxes. Under the GDPR, consent is "unambiguous" only with a clear affirmative action by the user, which does not happen when a user fails to un-tick a pre-ticked box.[10]

B. Enforcement in the United Kingdom

Regulators in the United Kingdom have also imposed a significant fine on a U.S. company for violation of privacy law. Following the Cambridge Analytica scandal involving the likely use of personal information from social media for political purposes,[11] the United Kingdom's Information Commissioner's Office fined Facebook £500,000 in October 2018 for violating the Data Protection Act 1998, the UK's pre-GDPR privacy law. [12] Facebook's violations involved unfair processing of data and failure to guard against unlawful processing by a third party.[13] The data were collected between 2013 and 2015 by means of application software (the App) created by Dr. Aleksandr Kogan which Facebook permitted Dr. Kogan and his company, Global Science Research, to operate in conjunction with the Facebook Platform.[14] The App collected data of Facebook users and Facebook friends of those users.[15] Although the App used the Facebook login

---

[7] *Id.*
[8] *Id.* "'[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR, *supra* note 1, art. 4 (11).
[9] *CNIL Decision*, *supra* note 6; GDPR, *supra* note 1, art. 4 (11).
[10] *CNIL Decision*, *supra* note 6; GDPR, *supra* note 1, art. 4 (11).
[11] See, e.g., John Hermann, *Cambridge Analytica and the Coming Data Bust*, N.Y. TIMES, Apr. 10, 2018, https://www.nytimes.com/2018/04/10/magazine/Cambridge-analytica-and-the-coming-data-bust.html.
[12] United Kingdom Information Commissioner's Office, *Data Protection Act 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice 24 October 2018*, https://ice.org.uk/action-weve-taken-/enforcement/facebook-ireland-ltd/ (last visited May 6, 2019).
[13] *Id.*
[14] *Id.* at 9
[15] *Id.*

to request permission from users to obtain access to their data, no such permission was obtained from Facebook friends of those users.[16] Although 300,000 Facebook users used the App, the total number of people around the world whose data were collected through the App was probably 87 million, one million of whom were probably in the United Kingdom.[17] Dr. Kogan and his company shared the data with various third parties, including SCL Elections Limited, which controlled Cambridge Analytica.[18] It is likely that at least some of the data were used in connection with political campaigns.[19] The Information Commission's Office found that UK privacy law was breached in that Facebook friends whose data were being collected were not adequately informed of the collection and were not asked to consent to the collection.[20] Moreover, Facebook also violated privacy law by failing to take steps to ensure that data collected by the App were processed in accordance with Facebook's Platform Policy and in accordance with assurances made by Dr. Kogan that the data would be used only for research.[21] Although the fine of £500,000 was the maximum under the law in effect at the time of the violation, the Information Commission's Office stated that a higher penalty would have been reasonable, given the severity of the offense.[22]

C. Other Enforcement Measures

Because many large U.S. tech companies have their European headquarters in Ireland, the Irish Data Commissioner's Office is their lead privacy regulator.[23] As of February 2019, it had sixteen investigations underway.[24] Seven of those investigations involved Facebook,[25] including a number of data breach notification cases,[26] one of which involved Twitter.[27] In a case with potential antitrust as well as data protection issues, the Irish regulatory authority examined the sharing and merging of personal data between Facebook and its subsidiaries, WhatsApp and Instagram.[28] Data protection practices of other U.S. tech companies were also under review in

---

[16] *Id*. at 10.
[17] *Id*. at 12.
[18] *Id*.
[19] *Id.*
[20] *Id*. at 15.
[21] *Id*. at 18.
[22] *Id*. at 5.
[23] The supervisory authority of the main establishment of the controller acts as the lead supervisory authority for cross-border processing of data. GDPR, *supra* note 1, art. 56 (1).
[24] *See, e.g., Irish DPC opened seven different probes against Facebook*, Feb. 1, 2019, https://iapp.org/news/a/irish-dpc-opened-seven-different-probes-against-Facebook (last visited Feb. 25, 2019).
[25] *Id*.
[26] *See, e.g.*, Irish Data Protection Commission, *Facebook Data Breach – Commencement of Investigation*, Oct. 3, 2018, https://www.dataprotection.ie/en/news-media/press-releases/facebook-data-breach-commencement-investigation (last visited Apr. 23, 2019); Irish Data Protection Commission, *Data Protection Commission opens statutory inquiry into Facebook*, Dec. 17, 2018, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-facebook (last visited Apr. 23, 2019).
[27] *See, e.g., Irish data watchdog investigates Twitter over privacy rules breach*, Jan. 25, 2019, https://www.reuters.com/article/us-twitter-cyber-ireland/irish-data-watchdog-investigated-twitter-over-privacy-rules-breach-ifUSKCN1PJ28G (last visited Feb. 25, 2019).
[28] *See, e.g.*, Irish Data Protection Commission, *Data Protection Commission statement on proposed integration of Facebook, WhatsApp and Instagram*, Jan. 28, 2019, https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-proposed-integration-facebook (last visited Apr. 23, 2019).

Ireland, including those of Apple and LinkedIn.[29] In Belgium, Facebook appealed a court order forcing it to stop tracking the online activities of its users and others.[30] Facebook was also under scrutiny by the European Commission and a number of European national consumer protection authorities for misleading information in its terms of service.[31]

II. Enforcement of Competition Law by the European Commission

The European Commission has been active in enforcing EU competition law against Google. Article 102 of the Treaty on the Functioning of the European Union prohibits abuse of a dominant market position.[32] In three separate cases, the Commission fined Google a total of over €8 billion for abusing its dominant position in markets for online services.

A. Google Shopping

In June 2017, the European Commission fined Google €2.42 billion for abusing its market dominance by favoring its comparison shopping service, Google Shopping, over rivals in general internet search results.[33] Google's search engine had a market share of at least 90% in most EU countries and the Commission found high barriers to entry in these markets.[34] Since the beginning of the abuse, Google's comparison shopping service had increased it traffic 45-fold in the United Kingdom, 35-fold in Germany, 19-fold in France, 29-fold in the Netherlands 17-fold in Spain and 14-fold in Italy.[35]

B. Google Android

---

[29] *See, e.g., Irish DPC opened seven different probes against Facebook*, Feb. 1, 2019, https://iapp.org/news/a/irish-dpc-opened-seven-different-probes-against-Facebook (last visited Feb. 25, 2019).

[30] *See, e.g., Facebook to Fight Belgian Ban on Tracking Users (and Even Non-Users)*, Mar. 27, 2019, https://www.bloomberg.com/news/articles/2019-03-27/facebook-attack-of-belgian-order-on-user-tracking-gets-hearing (last visited Apr. 23, 2019).

[31] *See, e.g., Facebook Bends to EU Pressure on 'Misleading' Fine Print*, WALL ST. J., Apr. 9, 2019, https://www.wsj.com/articles/facebook-bends-to-eu-pressure-on-misleading-fine-print-11554804346?mod=hp_major-pos16.

[32] TFEU art. 102 provides:

"Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in:

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts."

[33] European Commission, *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service*, europa.eu/rapid/press-release_IP-17-1784_en.htm (last visited May 5, 2019).

[34] *Id.*

[35] *Id.*

In July 2018, the European Commission fined Google €4.34 billion for illegal practices which strengthened its dominant position in general internet searches.[36] The Commission repeated its finding from the Google Shopping case the previous year, that Google's search engine had a market share of at least 90% in most EU countries and that there were high barriers to entry in these markets.[37] It found that Google had imposed three types of restrictions on manufacturers of Android mobile devices that ensured that internet search traffic went to Google's search engine, thus depriving rivals an opportunity to compete and denying consumers the benefits of competition.[38] In Europe, approximately 80% of smart mobile devices run on the Android operating system.[39] All three restrictions were found to be abuses of Google's dominant market position.[40] The first restriction was a requirement that manufacturers pre-install the Google search app and the Chrome browser as a condition for obtaining a license to the Google Play Store. The second practice involved payments by Google to manufacturers and mobile network operators obligating them to pre-install the Google search app, and no other search app, on their mobile devices.[41] The third practice involved a restriction in agreements with manufacturers to pre-install Google apps. The restriction involved exclusionary practices involving versions of Android known as "Android forks."[42] When Google develops a new version of Android, it publishes the computer source code online.[43] The published version, however, covers basic features of the operating system which can then be used by other software developers to create versions of Android known as "Android forks."[44] An example of an Android fork is Amazon's "Fire OS."[45] Google's proprietary Android apps and services, however, are not publicly available.[46] Manufacturers and mobile network operators who want to obtain Google's proprietary Android apps and services must enter into licensing contracts which impose a number of restrictions, one of which prohibits a licensee from selling any devices running Android forks.[47]

C. Google AdSense

In March 2019, the European Commission fined Google €1.49 billion for illegally imposing contractual restrictions on third-party websites using a Google service known as AdSense.[48] Websites for newspapers, travel site aggregators and others often have an embedded

[36] European Commission, *Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine*, europa.eu/rapid/press-release_IP-18-4581_en.htm (last visited May 5, 2019).
[37] *Id*.
[38] *Id*.
[39] *Id*.
[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] *Id*.
[46] *Id*.
[47] *Id*.
[48] European Commission, *Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising,* europa.eu/rapid/press-release_IP-19-1770_en.htm (last visited May 5, 2019).

search function.[49] Such websites are known as "publisher" websites.[50] AdSense is an online search advertising intermediation service which delivers advertising that appears alongside search results.[51] The Commission determined that Google had at least 85% of the online search advertising intermediation service market.[52] Google had restrictive clauses in its AdSense contracts with publisher websites. The restrictions took three forms. Between 2006 and 2009, the contracts had exclusivity clauses prohibiting publishers from placing any search advertising delivered by AdSense competitors on search result pages.[53] Starting in 2009, the exclusivity clauses were replaced by "premium placement" clauses, requiring publishers to reserve the most profitable space on their search result pages for advertising delivered by AdSense.[54] Also starting in 2009, publishers were required to seek written approval from Google before making changes to the way in which non-AdSense-delivered ads were displayed.[55] Google ceased the restrictive practices in 2016 after the Commission issued a Statement of Objections concerning the case.[56] In March 2019, the Commission found the restrictions to be abuse of Google's dominant position in the market for online search advertising intermediation.[57]

III. The Movement to Combine Data Protection and Competition Analyses

The possibility of evaluating business behavior under both data protection and competition analyses has been considered by regulators on both sides of the Atlantic for years. For example, during the Federal Trade Commission's evaluation in 2007 of Google's acquisition of DoubleClick, two Commissioners wrote separate opinions raising concerns about consumer privacy as part of their analysis of the merger. Although Commissioner Jon Liebowitz concurred with the majority's approval of the combination of the two companies, he wrote that "rampant tracking of our online conduct, as well as the resulting consumer profiling and targeting raises critical issues about the companies' disclosures, the depth of consumers' understanding and control of their personal information and the security and confidentiality of the massive collection of sensitive personal data."[58] In her dissent, Commissioner Pamela Jones Harbour applied a broader approach than the majority by emphasizing that the merger would combine large amount information regarding consumer behavior on the Internet that involved an interplay between competition and consumer protection issues.[59] She also noted that because of the "network effect" arising when a service increases in value as more people use it, the merger of the personal data held by the two companies

[49] *Id*.
[50] *Id*.
[51] *Id*.
[52] *Id*.
[53] *Id*.
[54] *Id*.
[55] *Id*.
[56] *Id*.
[57] *Id*.
[58] *Concurring Statement of Commissioner Jon Leibowitz, Google/DoubleClick*, FTC File No. 071-0179, https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-jon-leibowitz-google/doubleclick-matter/071220leib_0.pdf.
[59] *Dissenting Statement of Commissioner Pamela Jones Harbour, In the matter of Google/DoubleClick*, FTC File No. 071-0170, http://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf at 4.

make it difficult for a competitor to challenge the combined firm.[60] If the combination leads to a reduction in the number of online search competitors, she reasoned, it will reduce consumer choice and possibly reduce incentives for search firms to compete based on privacy protections.[61] Her dissent concluded by stating that the unique confluence of competition and consumer protection issues in this case should have been a call to action for the FTC, because of its expertise in both areas.[62]

For years, government officials in Europe have also considered links between privacy and competition law. For example, Joaquin Almunia, Vice President of the Commission of the European Union, gave a speech on competition law and data privacy in 2012, noting that a dominant company could violate privacy laws to gain an advantage over competitors.[63] Although at the time of his speech the Commission had not yet handled a case in which personal data were used to breach EU competition law, he mentioned that the most prominent case involving both subjects was the Commission's review of the merger between Google and DoubleClick, which was approved solely on the basis of competition law, without considering issues involving data protection.[64]

The European Data Protection Supervisor, whose responsibilities include data protection across EU institutions, has also been instrumental in stimulating a dialog regarding connections between privacy and competition law, both by sponsoring a conference in Brussels in 2013[65] and by publishing of a forty-page report, titled "Preliminary Opinion," in 2014.[66] The report set forth an analysis of how personal information has become the fuel for the digital economy, the connections between laws governing data protection, competition and consumer protection, and the need for coordinated enforcement and further discussion among regulators.[67]

IV. The Call for Parallel Investigations in the United Kingdom

Connections between data protection and competition law have also been considered in the United Kingdom. In a report released in February 2019, a Committee of the House of Commons cited both data protection and competition law in making recommendations regarding regulation of large tech companies.[68] The report focused largely on Facebook and its role in the Cambridge Analytica scandal involving use of Facebook users' data without their knowledge or consent, and the use of Facebook to spread disinformation for political purposes. In connection with its

---

[60] *Id*. at 5.
[61] *Id*. at 10, note 25.
[62] *Id*. at 12.
[63] Joaquin Almunia, *Competition and personal data protection,* at http://Europa.eu/rapid/press-release_SPEECH-12-860_en.htm (last visited Apr. 28, 2019.)
[64] *Id.*
[65] *See, e.g.*, European Data Protection Supervisor, *Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data*, 2014 O.J. (C 225/6) 7.
[66] European Data Protection Supervisor, *Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf.
[67] *Id*.
[68] House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report,* at https://publications.parliament/uk/pa/cm201719/smselecct/cmcumeds/1719/1719.pdf (last visited May 7, 2019).

investigation, the Committee obtained information from a lawsuit against Facebook in a California state court by U.S.-based app developer Six4Three.[69] The lawsuit alleged that Facebook overrode its users' privacy settings in order to transfer data of users and their Facebook friends to app developers to encourage them to create services on its platform.[70] Moreover, Six4Three alleged that Facebook used access to data in an anticompetitive way, either by charging the successful app developer a higher fee or by removing access when the developer became a potential competitor through its success.[71] The report recommended that the United Kingdom's Information Commissioner's Office investigate possible violations of data privacy and competition law.[72] The report also recommended that the United Kingdom's antitrust agency, the Competitions and Market Authority, conduct a comprehensive audit of the advertising market on social media to determine whether Facebook had been involved in any anti-competitive conduct, including unfairly using a dominant market position to decide which businesses should succeed or fail.[73] The report emphasized the seriousness of the company's behavior by stating that "[c]ompanies like Facebook should not be allowed to behave like 'digital gangsters' in the online world, considering themselves to be ahead of and beyond the law."[74]

V. Combined Analysis in the Facebook Case in Germany

The first formal connections between data protection and competition law in an enforcement action were made in February 2019 by Germany's Federal Cartel Office, the country's top enforcer of competition law, in a case against Facebook. [75] The investigation which began in 2016 examined the company's collection of personal information about Facebook users from both (1) Facebook-owned services, including WhatsApp and Instagram, and (2) websites operated by third parties. Facebook transferred the data from these sources to its users' accounts, thus increasing the amount of personal information in each user's Facebook dossier.[76]

In addition to services aimed at individuals, the company offered website operators, developers, advertisers and other businesses a selection of free tools and products known as "Facebook Business Tools."[77] The services included social plugins in the form of "Like" or "Share" buttons, and other analytics services implemented through "Facebook pixel" or mobile "software development kits."[78] When a Facebook user visited a third party website containing a "Like" or "Share" button, the user's data would flow to Facebook even though the user did not

---

[69] *Id*. at 26.
[70] *Id*. at 42.
[71] *Id*.
[72] *Id*.
[73] *Id*.
[74] *Id*. at 91.
[75] Bundeskartellamt, *Press Release, Bundeskartellamt prohibits Facebook from combining user data from different sources,* https://www.bundesdartellamt.de/SharedDocs/Publikation/EN?pressemitteilungen/2019/07_02_2019_Facebook.pdf?blob=publicationFile&v=2 (last visited Apr. 27, 2019). [hereinafter *BKA Press Release*]
[76] *Id.*
[77] Bundeskartellamt, *Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing,* https://www.bundesdartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/blob=publicationFine&v=4 at 2 (last visited Apr. 27, 2019). [hereinafter *BKA Case Summary*].
[78] *Id*. at 3.

scroll over or click on the button.[79] Merely visiting a third party website that used "Facebook Analytics," however, would cause the user's data to flow to Facebook, regardless of whether a Facebook symbol was visible on the page.[80] Accordingly, users were not aware of Facebook's collection of information about their visits to third party websites.[81]

The Cartel Office found that Facebook's aggregation of personal information from multiple sources had allowed it to build a database for each user and thus gain market power.[82] As of December, 2018, its share of the German market for social networks was more than 95% for daily active users and more than 80% for monthly active users.[83] Competition was in decline. German social networks, including StudiVZ, SchullerVZ and Lokalisten, had left the market by 2017.[84] Moreover, Facebook's competitor, Google+, announced that it was shutting down its social network in 2019. Other services including Snapchat, YouTube, Twitter, Linkedin and Xing offer only part of the services of a social network and therefore were not part of the relevant market.[85] Accordingly, German Facebook users could not switch to other social networks. The only choice they had was either to accept Facebook's terms of service or refrain from using a social network.[86]

The Cartel Office found that Facebook's collecting, using and merging data in a user account constituted an abuse of a dominant market position in violation of German competition law.[87] The type of abuse, known as an exploitative abuse, takes place when a dominant company uses exploitative practices to the detriment of the other side of the market, in this case consumers who used Facebook.[88] In this situation, German competition law is applied in cases where one party is so powerful that it is able to dictate the term of the contract and the contractual autonomy of the weaker party is eliminated.[89] In addition, an exploitative abuse occurs when the practices impede competitors, in this instance from being able to amass a treasure trove of personal data.[90] The Cartel Office stated that its application of an exploitative abuse analysis under competition law corresponded to the approach taken by the German Federal Court of Justice.[91]

The Cartel Office also examined the relation between German competition law and European data protection principles.[92] In doing so, it maintained regular contact with German data protection authorities who supported the view that data protection law could be enforced by governmental authorities other than data protection regulators, and that such enforcement in coordination with competition law was appropriate.[93] Because Facebook bases its European

[79] *BKA Press Release*, *supra* note 75, at 3.
[80] *Id*.
[81] *Id*.
[82] *BKA Press Release*, *supra* note 75, at 2.
[83] *Id.*
[84] *BKA Case Summary*, *supra* note 77, at 6.
[85] *Id*.
[86] *BKA Press Release*, *supra* note 75, at 2.
[87] *Id*.
[88] *Id.* at 3.
[89] *BKA Case Summary*, *supra* note 77, at 8.
[90] *Id*.
[91] *Id.* at 7.
[92] *Id*. at 8.
[93] *Id*. at 9.

operations in Ireland, the Cartel office also briefed the Irish data protection authority about the case.[94]

In its analysis under data protection law, the Cartel Office considered whether Facebook's processing of data obtained from third parties had a lawful basis under data protection law. Three possibilities were considered: processing pursuant to consent by the data subject,[95] processing necessary for the performance of a contract with the data subject,[96] and processing necessary for the purposes of Facebook's legitimate interests.[97] Based upon its analysis that Facebook had a dominant market position, the Cartel Office concluded that users did not give effective consent as required by data protection law.[98] Secondly, the Cartel Office stated that the justification for processing necessary for the performance of a contract must be interpreted narrowly, otherwise a business would be entitled to unlimited processing solely on the basis of its business model.[99] In this instance, Facebook's processing of data from third party sources was neither required for offering the social network nor for monetizing the network through personalized advertising, as a personalized network could also be based on the data generated by the network itself.[100] Finally, the Cartel Office rejected the notion that the processing was justified as being necessary for Facebook's legitimate interests, because those interests were outweighed by other interests of Facebook users.[101] This part of the analysis overlapped with the consent analysis, as the emphasis was on Facebook's dominant bargaining power over its users and their reasonable expectations.[102]

In reaching its conclusion, the Cartel Office noted that both data protection law and competition law involve assessments which are similar when analyzing an unbalanced negotiation.[103] Its order prohibited Facebook from collecting and using data from third party sources without users' consent, and the combination of such data with Facebook data for purposes related to the social network.[104] Facebook was given four months to present a plan for the adjustments and twelve months to complete implementation of the changes.[105] Facebook appealed the decision to the Dusseldorf Higher Regional Court.[106]

---

[94] *Id*. *See supra* note 23.
[95] GDPR provides that processing is lawful if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes;" GDPR, *supra* note 1, art. 6(1)(a).
[96] GDPR provides that processing is lawful if "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;" GDPR, *supra* note 1, art. 6(1)(b).
[97] *BKA Case Summary, supra* note 77, at 10. GDPR provides that processing is lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." GDPR, *supra* note 1, art. 6(1)(f).
[98] *BKA Case Summary, supra* note 77, at 10. GDPR provides that "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;" GDPR, *supra* note 1, art. 4(11).
[99] *BKA Case Summary, supra* note 77, at 10.
[100] *Id*.
[101] *Id*.
[102] *Id*.
[103] *Id*. at 11.
[104] *Id*. at 12.
[105] *Id*.
[106] *Id*.

VI. Analysis of the Facebook Decision Using a Traditional Approach to EU Competition Law

Professor Renato Nazzini of King's College London has criticized the German Cartel Office's Facebook decision as blurring the boundaries between competition and data protection law, "depriving competition policy of its distinct identity."[107] While acknowledging that the Cartel Office was applying German, rather than EU, competition law, Professor Nazzini considered the extent to which the Cartel Office's reasoning was relevant to an assessment of harm under a traditional application of EU competition law. [108] He considered both exploitative theories of harm and exclusionary theories of harm.

Professor Nazzini characterized the Cartel Office's decision as finding exploitative abuse in Facebook's imposition of terms on users that were a manifestation of market power or which were inappropriate given that the constitutional rights involved include the right to information self-determination.[109] In other words, the harm was to the rights of Facebook users. Under his traditional interpretation of EU law, however, the finding of an exploitative abuse by a business in a dominant position must include a finding of competitive harm, which would not necessarily be present when there was a mere breach of data protection law.[110] He concluded that the Cartel Office's Case Summary did not provide an adequate basis under EU law for a finding that the exploitative harm caused by Facebook's conduct was competitive harm.[111]

With respect to exclusionary theories of harm, Professor Nazzini cited language in the Cartel Office's Case Summary finding that Facebook impeded competitors because it gained access to third party sources of data inappropriately combined with data in user accounts, thus gaining an unlawful competitive edge that increased barriers to entry.[112] He concluded, however, that it was not clear whether this finding as described in the Case Summary was supported by sufficient evidence to demonstrate exclusionary abuse under EU competition law.[113]

VI. An Adaptive Approach to EU Competition Law in the Digital Era

In contrast to Professor Nazzini's traditional approach which was narrowly focused on harm to competition, a report prepared for the European Commission in April 2019 recommended that traditional methods of applying competition law should be modified when applied to businesses operating in the digital economy.[114] Among the report's recommendations were modifications to standards of harm, definitions of markets, measurements of market power and

---

[107] Renato Nazzini, *Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision*, at https://www.competitionpolicyinternational.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-4-Full.pdf at 7.
[108] *Id.* at 2.
[109] *Id*.
[110] *Id*. at 4.
[111] *Id*. at 5.
[112] *Id*.
[113] *Id*.
[114] Heike Schweitzer, Jacques Cremer and Yves-Alexandre de Montjoye, *Competition Policy for the Digital Era*, available at ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

burdens of proof. For example, the report recommended that even when consumer harm cannot be precisely measured, activities by a dominant business aimed at reducing competitive pressure should be prohibited, in the absence of clearly documented consumer welfare gains.[115] There should be less emphasis on market definition and more emphasis on theories of harm and identification of market strategies.[116] When there is a highly concentrated market and high barriers to entry, competition law should err on the side of disallowing potentially anti-competitive conduct and place a burden on an incumbent business to show that its conduct is pro-competitive.[117] The report noted an interdependence between competition law and data protection law, in that data protection law affects competition and market power affects reasonably available data choices of consumers.[118] Moreover, there should be an integrated approach in which competition law takes data protection law into account, and data protection implementation considers matters relating to competition.[119] The report included mention of the German Cartel Office's Facebook decision as an example of the interdependence between the two areas of law.[120] The report made the point that Facebook's market dominance is relevant for assessing the validity of a user's consent to Facebook's term of use[121] and that Facebook's market power is also relevant to a balancing of Facebook's interests against the fundamental rights of a Facebook user[122]

Conclusion

Activities of large U.S. tech companies that collect and use massive amounts of personal data involve issues of both privacy law and competition law. Market dominance is relevant with respect to a number of data protection issues under EU law, including the validity of consent by data subjects and a balancing of interests to determine whether there is a lawful basis for processing. The decision of German Cartel Office in the Facebook case demonstrates the value of an enforcement system which combines the principles from the two areas of law. Moreover, as set forth in the report prepared for the European Commission in April 2019, regulators need to adjust the analytical tools, methodologies and theories of harm to better fit the new market reality.[123]

[115] *Id*. at 3.
[116] *Id*.
[117] *Id*. at 4.
[118] *Id*. at 73.
[119] *Id*. at 77.
[120] *Id*. at 79.
[121] *Id*.
[122] *Id*.
[123] *Id*. at 125.