Northwestern Journal of International Law & Business

Volume 39
Issue 1 *Fall*

Fall 2018

The Tipping Point – Reevaluating the ASNEF-EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach

Olivia Altmayer

Vol. 39, No. 1
Northwestern Journal of International Law & Business

THE TIPPING POINT – REEVALUATING THE *ASNEF-EQUIFAX* SEPARATION OF COMPETITION OF DATA PRIVACY LAW IN THE WAKE OF THE 2017 EQUIFAX DATA BREACH

Olivia A. Altmayer

Abstract: Contrary to the Court of Justice for the European Union's decision in the Asnef-Equifax case, in a world of big data, it is inefficient and ineffective to treat EU competition law and EU data protection law as entirely separate legal considerations. Reevaluating this stance is critical in sectors where customer data is highly sensitive, and therefore highly valuable to those who steal it, particularly for the financial and healthcare sectors. Looking forward, companies that store and use biometric data will have to be similarly scrutinized.

To correct this problem, the EU has numerous paths it can take: (a) continue as is, treating competition and data protection as separate legal considerations, (b) enact a new body of regulatory law to specifically deal with data protection and competition, or (c) begin using existing competition law, specifically Article 101 of the TFEU, to address data protection concerns. This paper will argue that to best serve the interests of all relevant players – government, businesses, and consumers – option (c) is the optimal choice. Additionally, in implementing this change, the EU can use the FRAND patent and competition law precedence in devising a new data protection and competition framework.

TABLE OF CONTENTS

I. INTRODUCTION

Since 2006 when the Court of Justice decided the *Asnef-Equifax* case[1] for the European Union (EU), the landscape of data security has changed drastically. Of the eighteen largest data breaches of all time, only two occurred before 2010 and both were tied to the same hacker.[2] Of the breaches that have occurred since, the 2017 Equifax breach is thought to be the most dangerous because the data stolen from an estimated 143 million consumers included social security numbers, which are characterized as extremely sensitive data.[3] Breaches that involve such a vast swath of sensitive consumer information pose a real threat to economic security.[4] It is clear, then, that governments need to take additional steps to combat a heightened threat to the security of sensitive information. This is especially true for credit and medical information which are of most value to hackers and therefore most at risk.[5]

One possible approach to increasing the protection on this sensitive data is incorporating data protection analysis into competition law review when private companies propose or challenge mergers. There is precedent for this sort of combined approach regime with patents and competition law in the EU. The situation appears ripe for creative solutions when it comes to big companies and the protection of consumer data and information. The EU is taking steps to drastically increase the strength of its data protection laws, with the introduction of General Data Protection Regulation, which took effect in May 2018. During the same time frame, the European Commission has also increased competition law scrutiny on companies operating in the EU. Adding a review of data protection policies and procedures would be a good way for the government to mitigate the problem of increased data security threats and make the data and information of European consumers safer. However, it is much less clear that such a regime would be embraced or effective in other jurisdictions, especially the United States.

---

[1] Case C-238/05, Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL and Administación del Estado Asociación de Usuarios de Servicios Bancarios (Ausbanc), 2006 E.C.R I-11125 [hereinafter Asnef-Equifax].

[2] Computer hacker Albert Gonzalez was held responsible for both the 2006 TJX Companies, Inc. breach and the 2008 Heartland Payment Systems breach. Taylor Armerding, *The 18 Biggest Breaches of the 21st Century*, CSO ONLINE https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (last updated Dec. 20, 2018).

[3] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth & Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N. Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?_r=0.

[4] *Id.*

[5] Credit information is tied to an individual through their social security number or other national identification number. Aatif Sulleyman, *NHS Cyber Attack: Why Stolen Medical Information Is So Much More Valuable Than Financial Data*, INDEPENDENT (May 12, 2017), http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html.

This note focuses on an observable intersection of data protection and competition law to create a more efficient regulatory environment with the goal of offering consumers the best protection for their personal data at the least cost for the companies storing and processing that data. Part I will review competition law and its recent developments in Europe. Part II will focus on data protection law's development in the EU and the US. Part III will analyze the decision made by the Court of Justice for the EU in the 2006 *Asnef-Equifax* case. Part IV will propose possible choices for the EU in combating the possible failings of the current system. Finally, Part V will serve as the conclusion and discuss the optimal strategy going forward for the EU in this area of the law.

II. COMPETITION LAW

A. History of Competition Law

In preparing to discuss the intersection of competition law and data protection law in the EU at present, it is first important to review the origins and purposes of both bodies of law. Competition law is the older of the two and can trace its roots back to ancient times. There is evidence that competition law dates back to ancient Greece[6] and Egypt.[7] The modern iteration of competition law began in the late 19th century in the United States with the passage of the Sherman Act, which focused on preserving the competitive market and benefiting consumers through fair prices.[8]

The Chicago School approach to competition law has been dominant in both the United States and Europe since the 1970s.[9] This approach requires an assessment of market structure, company behavior, and company performance in the market to determine whether a company's conduct violates competition law.[10] Additional competition law concerns include protecting the free market from "artificial restraints,"[11] ensuring the efficient allocation of resources, and recognizing barriers to entry for would-be market players.[12] Horizontal sharing of information is one of the ways that companies reduce competition in the market, which was the point of concern in the *Asnef-Equifax* case[13] and is a primary component of the credit bureau

---

6 THE EC LAW OF COMPETITION 5 (Jonathan Faull & Ali Nikpay eds., 2d ed. 2007).

7 Lorenzo F. Pace, EUROPEAN ANTITRUST LAW: PROHIBITIONS, MERGER CONTROL AND PROCEDURES 3 (2007).

8 Frederic Sautet, *The Shaky Foundations of Competition Law*, N.Z. L.J. 186, 189-90 (2007).

9 THE EC LAW OF COMPETITION, *supra* note 6, at 8.

10 *Id.*

11 Erich Hoppmann, *Workable Competition - The Development of an Idea on the Norm for the Policy of Competition*, 13 ANTITRUST BULL. 61 (1968).

12 Pace, *supra* note 7, at 39.

13 Asnef-Equifax, *supra* note 1, at I-11125.

industry.[14]

B. Competition Policy in the EU

Competition policy in the European Union began in March of 1957 with the Treaty of Rome, in which Articles 85 and 86 of the European Economic Community (EEC) were some of the first treaty provisions to have a direct effect on the EU.[15] As of 2007, these provisions are Articles 101 and 102[16] of the Treaty on the Functioning of the European Union (TFEU).[17] In 1962, the European Commission, the EU's politically independent executive body,[18] received the direct power to enforce competition law under Regulation 17, later superseded by Regulation 1/2003.[19] The Commission is "responsible for the implementation and orientation of Community competition policy."[20] The European Court of Justice (ECJ), the highest court in the European Union, ensures that the interpretation and application of EU law is consistent across member states.[21] In the competition law arena, the ECJ ensures stability of the law and maintains preeminence over national laws. The ECJ has also interpreted Articles 85 and 86 to be real applicable law and not merely policy guidelines.[22] The ECJ is further responsible for protecting the rights of private individuals under antitrust law.[23] Together, the European Commission and the ECJ give teeth to the European Union's competition policy.

The European Commission and the ECJ have two avenues to enforce competition law in the EU. The first is enforcement through merger control, and the second is legal action for violation of Article 101 or 102. The European Commission is tasked with assessing the effects of a merger on the market and has the sole power to make decisions regarding whether a proposed merger is in compliance with Regulation 139/04.[24] The two phases of merger review are: (i) assessment of whether the market concentration may create a threat to competition; and if a threat is present (ii) a more

---

[14] Marc Rothemund & Maria Gerhardt, *The European Credit Information Landscape: An analysis of a survey of credit bureaus in Europe*, ECRI INDUSTRY SURVEY 2 (Jan. 2011).

[15] THE HISTORICAL FOUNDATIONS OF EU COMPETITION LAW 1 (Kiran Klaus Patel & Heike Schweitzer eds., 2013).

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

[17] THE HISTORICAL FOUNDATIONS OF EU COMPETITION LAW, *supra* note 15, at 1.

[18] EUROPEAN COMMISSION, https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en (last visited Nov. 4, 2017).

[19] THE HISTORICAL FOUNDATIONS OF EU COMPETITION LAW, *supra* note 15, at 1.

[20] PACE, *supra* note 7, at 199.

[21] COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU), https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Nov. 4, 2017).

[22] THE HISTORICAL FOUNDATIONS OF EU COMPETITION LAW, *supra* note 15, at 10.

[23] PACE, *supra* note 7, at 206.

[24] *Id.* at 357.

thorough assessment of the threats to competition which may culminate in a decision to block the merger.[25] Article 21(2) of Regulation 139/04[26] serves as a check on this review power, saying that the Commission's exclusive power is subject to review by the Court of Justice.[27] Regulation 1/2003[28] specifically grants jurisdiction to national courts to hear antitrust cases.[29] Finally, if the European Commission finds that there has been an antitrust infringement, then the Commission should propose measures to end the infringement.[30] If that fails, then the Commission is to record the infringement in a reasoned decision.[31] Therefore, both the courts and Commission can impose penalties for uncured antitrust infringement.[32]

Competition law in Europe, "the set of laws which ensure that competition in the marketplace is not restricted in a way that is detrimental to society," is distinct from U.S. antitrust law.[33] European case law conveys a special responsibility on firms holding a dominant market position to make sure that their conduct does not distort or lessen competition.[34] Governmental interventions under competition law are to only occur when "they can be shown to maximize welfare overall."[35] Therefore, especially in Europe, one can consider competition law as a means to protect social welfare.[36]

C. Recent Developments in EU Competition Policy

The European Commission has been very active recently in bringing competition law enforcement actions against tech giants like Facebook, Google, Microsoft, and Apple. By doing so, they are walking the fine line between addressing concerns of market failures and public policy, risking the real possibility of suppressing innovation through excessive intervention.[37]

---

[25] *Id.*

[26] Council Regulation 139/2004 of Jan. 20, 2004, On the Control of Concentrations between Undertakings (the EC Merger Regulation), 2004 O.J. (L 24) 1, 17 [hereinafter Merger Regulation].

[27] Pace, *supra* note 7, at 357.

[28] Council Regulation 1/2003 of Dec. 16, 2002, On the Implementation of the Rules on Competition Laid down in Articles 81 and 82 of the Treaty, 2003 O.J. (L 1) 1.

[29] Pace, *supra* note 7, at 310.

[30] *Id.* at 209.

[31] *Id.*

[32] *Id.* at 210.

[33] Massimo Motta, COMPETITION POLICY: THEORY AND PRACTICE 30 (2004).

[34] *Communication from the Commission – Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings*, COM (2009) 2009/C 45/02 final (Feb. 24, 2009), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN.

[35] THE HISTORICAL FOUNDATIONS OF EU COMPETITION LAW, *supra* note 15, at 2.

[36] *See* Joseph F. Brodley, *The Economic Goals of Antitrust: Efficiency, Consumer Welfare, and Technological Progress*, 62 N.Y.U. L. REV. 1020, 1025 (1987).

[37] Peter Alexiadis, *Forging a European Competition Policy Response to Online Platforms*, 18 BUS. L. INT'L (IBA) 91, 93-94 (May 2017).

The underlying principle for this increased scrutiny goes back to the European idea that when a firm is dominant in a market, it faces a heightened responsibility for ensuring that its actions do not lessen competition.[38] Increasingly, the European Commission has been looking for anti-competitive conduct related to the treatment of data by these technology companies, in part because of a drastic increase in the data volume processed and held and a substantial increase in electronic communication.[39]

The first big case was the review of the Google and DoubleClick merger, which the European Commission cleared after going through the merger review process in 2007.[40] At this point in time Google was the most popular internet search engine and was offered to users for free, and DoubleClick was a U.S. entity that sold "ad serving, management and reporting technology worldwide to website publishers, advertisers and advertising agencies."[41] What concerned the European Commission was the potential foreclosure effect on the online advertising market.[42] However, the transaction ended up being approved because the Commission found that the switching costs were not cost-prohibitive for publishers and customers to switch between providers within the online advertisement market.[43] The U.S. Federal Trade Commission (FTC) similarly cleared the transaction.[44] One FTC Commissioner, Pamela Jones Harbour, dissented to the majority decision because she felt that the decision did not adequately address the competition concerns and the privacy interests of consumers, but in this viewpoint she stood alone.[45]

The European Commission also reviewed Microsoft's acquisitions of Skype and LinkedIn. In 2011, the European Commission received notice that Microsoft was planning to acquire Skype.[46] The European Commission cleared this transaction because it decided that the common market would

---

[38] *Commission Communication*, *supra* note 34.

[39] Monika Kuschewsky & Damien Geradin, *Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges*, 37 WORLD COMPETITION L. & ECON. REV. 69 (2014).

[40] Summary of Commission Decision in Case COMP/M.4731 of 11 Mar. 2008, 2008 O.J. (C 184) 10.

[41] *Id*.

[42] *Id*. at 11-12.

[43] *Id*.

[44] Federal Trade Commission, Statement Concerning Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

[45] Pamela Jones Harbour, Dissenting Statement in the Matter of Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf.

[46] Prior Notification of a Concentration in Case COMP/M.6281 of 10 Sept. 2011, 2011 O.J. (C 268) 12.

not be significantly impacted as a result of the merger.[47] With Microsoft's 2016 acquisition of LinkedIn, the Commission was stricter. They only approved the deal subject to certain conditions.[48] First, LinkedIn software would have to be removable from Microsoft products.[49] Second, other professional social network services would have to still be operational on Microsoft products.[50] Finally, LinkedIn competitors would still have to be able to access the "Microsoft Graph" to help drive new subscribers to their own competing social networks.[51] Despite agreeing to allow this merger, conditional on the parties meeting the designated conditions, the European Commission acknowledged having a concern over the privacy effects of market concentration.[52] The worry, brought up at the very end of their decision, is that the privacy policies of the newly consolidated entity would become more relaxed as a result of decreased market competition.[53]

The European Commission also reviewed Facebook's proposed acquisition of WhatsApp in 2014.[54] At the time, the Commission cleared the transaction because the concentration of user data after the consolidation was thought to be a data protection issue, not a competition law issue, with the Commission specially writing that "any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of EU competition law rules but within the scope of EU data protection rules."[55] The Commission's investigation also revealed that consumers were increasingly concerned with the privacy and security of their personal information.[56]

The merger approval in 2014 did not actually end up closing the case for Facebook. In December 2016, the European Commission decided to review the decision and sent a Statement of Objections to Facebook, a formal step in an investigation by which the Commission alerts the company of the objections it is facing.[57] The specific claim was that during the 2014 merger

---

[47] Non-opposition to a Notified Concentration in Case COMP/M.6281 of 22 Nov. 2011, 2011 O.J. (C 341) 2.

[48] European Commission Press Release IP/16/4284, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Condition (Dec. 6, 2016), http://europa.eu/rapid/press-release_IP-16-4284_en.htm.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Commission Decision in Case M.8124, ¶ 350 (Dec. 6, 2016), http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.

[53] *Id.*

[54] Commission Decision in Case COMP/M.7217 (Oct. 3, 2014), http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.

[55] *Id.* at ¶ 164.

[56] *Id.* at ¶ 87.

[57] European Commission Press Release IP/16/4473, Mergers: Commission Alleges Facebook Provided Misleading Information about WhatsApp Takeover (Dec. 20, 2016),

review, Facebook provided misleading information about whether user accounts of both companies could be matched. In 2014, Facebook said it would not be able to do so, information which the Commission took into account when deciding to clear the transaction.[58] However, in August 2016, WhatsApp announced changes to its terms of service and privacy policy which allowed for the possibility of linking WhatsApp phone numbers with Facebook user identities, a direct contradiction to the 2014 claims of Facebook.[59] Because Facebook failed to provide correct information in 2014, the Commission imposed a €110 million fine[60] on the company in May 2017.[61] This was the first fine of its kind following the adoption of the 2004 Merger Regulation.[62]

Facebook is also facing a similar complaint in Germany. The Federation of German Consumer Organizations (VZBV), a German consumer agency, is investigating whether Facebook abused its dominant market position and breached German data protection rules through unlawful data sharing.[63] If German authorities find a violation of competition law through a non-market matter (data protection), that decision could pave the way for the EU to follow suit.[64] Competition Commissioner Margarethe Vestager has acknowledged as much, saying "it shouldn't only be the Commission doing things that are new in terms of developing competition law."[65]

Finally, there is precedent in the EU for using competition law to strengthen regulation for another body of law; specifically, competition law and patent law. In 2014 there were two cases, *Motorola v. Apple*[66] and *Samsung v. Apple*[67], which centered on something called "standards" which "ensure compatibility and interoperability of telecom networks and mobile

http://europa.eu/rapid/press-release_IP-16-4473_en.htm.

[58] *Id*.

[59] *Id*.

[60] *See* Merger Regulation, supra note 26, at 15. The Merger Regulation allows for the imposition of a fine up to 1% of the aggregated turnover of a company that intentionally or negligently provides incorrect or misleading information to the Commission.

[61] European Commission Press Release IP/17/1369, Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover (May 28, 2017), http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

[62] *Id.*

[63] Press Release, VZBV, VZBV Verklagt WhatsApp: Verbraucher Mussen Hoheit Über Daten Behalten (Jan. 30, 2017), www.vzbv.de/pressemitteilung/vzbv-verklagt-whatsapp-verbraucher-muessen-hoheit-ueber-daten-behalten.

[64] Nuria Boot & Georgios Petropoulos, *German Facebook Probe Links Data Protection and Competition Policy*, BRUEGEL BLOG (Mar. 14, 2016), http://bruegel.org/2016/03/german-facebook-probe-links-data-protection-and-competition-policy/.

[65] Foo Yun Chee, *German Regulator Wee Suited to Investigate Facebook: EU's Vestager*, REUTERS (Mar. 7, 2016), http://www.reuters.com/article/us-eu-facebook-antitrust/german-regulator-well-suited-to-investigate-facebook-eus-vestager-idUSKCN0W91OB.

[66] Commission Decision No. AT.39985, 2014 O.J. (C 344/06).

[67] Commission Decision No. AT.39939, 2014 O.J. (C 350/08).

devices."[68] Standards are composed of "standard-essential patents," which are distinct from ordinary patents because they are necessary for standards and implemented in nearly all of telecommunication devices.[69]

In *Motorola v. Apple*, Apple wanted to enter the mobile phone market and sought to license certain standard-essential patents from Motorola, which Motorola refused and for which it sought court ordered injunctions.[70] Apple defended itself saying that through its conduct, Motorola was violating competition law, specifically Article 102 of the TFEU.[71] This argument was successful. The EU Commission held that an injunction was unnecessary and no fines were ordered for Motorola's competition violation because of a lack of case-law precedent.[72]

In *Samsung v. Apple*, Samsung sought preliminary and permanent injunctions against Apple on the basis of some of its standard-essential patents.[73] The Commission viewed the conduct of Samsung between April 2011, when they initially sought the injunctions, and December 2012, when they withdrew the injunction actions, as possibly violating competition law under Article 102 of the TFEU.[74] In hearing these concerns from the Commission, Samsung made certain commitments so that no competition violation proceedings would continue.[75] Both cases represent competition law reaching out to impose limitations or requirements in another body of law, laying the groundwork for a similar interchange between competition law and data protection law.

III. DATA PROTECTION LAW

A. History of Data Protection Law

Data protection law, what it is and how it works, is equally important to understanding the proposal of this paper. Compared to competition law, data protection law is a much more recent development, and centers largely on the concept of privacy. In Europe, privacy is a fundamental right, similar to the right of "freedom of speech" in the United States.[76] It is important to note that there is no fundamental right of privacy in the United States.[77] Thus, EU

---

[68] Commission Decision No. AT.39985 at ¶ 5.

[69] *Id.* at ¶ 6.

[70] *Id.* at ¶ 11-12.

[71] See *id.* at ¶ 20.

[72] *Id.* at ¶ 24-25.

[73] Commission Decision No. AT.39939 at ¶ 12.

[74] *Id.* at ¶ 13.

[75] *Id.* at ¶ 14-20.

[76] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1170 (2000).

[77] McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 422 (2016).

data protection law derives from Europeans' fundamental right of privacy.[78]

Scholars made comparisons between intellectual property and personal information and data, and suggested that a property right should be granted to individuals by law much like intellectual property rights.[79] If personal information carried a property right, companies seeking to use that information could license it, but would also leave the individual the choice of whether to license.[80] No such property right exists in the U.S., but Europe took a rights-based approach to its data protection regulatory regime.[81] With society's increased reliance on technology, data protection concerns have come to the forefront as have questions about the best way to protect personal information.

The purpose of data protection law is to regulate and offer governmental protection to the increasing amount of digital data that moves between individuals, between organizations, or from an individual to an organization or vice versa.[82] Mechanisms invoked by this body of law to achieve its goals are minimum standards for organizational privacy policies and specific procedures for when a breach occurs. One complication that has continued to come up is data that flows between countries with different data protection laws, a function of the global interconnectivity provided by the internet.[83] Ensuring compliance with all data protection laws can be difficult, and most companies with international operations must comply with the strictest set of rules. Contradictions between such laws, especially between the lax and sometimes disjointed approach of the U.S. and the strict approach of the EU, make for a difficult and costly regulatory environment for international companies to navigate.[84]

B. Data Protection Policy in the EU

In the EU, data protection law has developed much more uniformly than it has in the United States.[85] This is partly a reaction toward Nazism and is also due to Europe's treatment of privacy as a fundamental right since the end of World War II.[86] Europeans experienced the havoc the Nazis and other fascists were able to wreak using census records, classified files – private and personal information – and understood the need for ensuring that such

---

[78] Tracie B. Loring, Comment, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 422 (2002).

[79] Samuelson, *supra* note 76, at 1126-27.

[80] *Id.* at 1129.

[81] *See* McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 668 (2012); Samuelson, *supra* note 76, at 1128.

[82] Cunningham, *supra* note 77, at 422.

[83] *Id.* at 434-35.

[84] *Id.* at 421.

[85] Loring, *supra* note 78.

[86] Samuelson, *supra* note 76, at 1170-71.

information is as well protected as possible.[87]

The German state of Hesse enacted the first comprehensive data protection law in 1970.[88] Afterwards, six unifying principles formed the foundation of further European data protection legislation.[89] These principles are openness, individual access and correction, collection limitation, use limitation, disclosure limitation, and security.[90] An example of the national legislation adopted during this time was the German *Bundesdatenschutzgesetz* of 1990, a federal data protection act that came out of a German Constitutional Court decision.[91]

The Organization for Economic Cooperation and Development (OECD) laid the foundation for the first broad reaching legal framework concerning data privacy.[92] In 1981 the Council of Europe held a convention for the protection of individuals specifically discussing automatic processing of personal data.[93] Both the Council of Europe and the OECD recognized a need for developing a framework that unified privacy and data principles.[94] The drafting and enacting of EU Council Directive 95/46/EC on October 24, 1995 saw their vision of a uniform data protection and privacy framework realized.[95]

The 1995 Directive's objective was to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[96] It defines personal data as information relating to an "identified or identifiable" person (the "data subject"), who is anyone who can be identified by reference to "an identification number or to one or more factors specific to . . . physical, physiological, mental, economic or social identity."[97] Also important for the regulation is the "controller" of personal data which can be a natural person, public authority, agency or other entity that "determines the purposes and

---

[87] Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 609-10 (2007).

[88] Helge Seip, *Data Protection, Privacy and National Borders*, *in* 25 YEARS ANNIVERSARY ANTHOLOGY IN COMPUTERS AND LAW 67, 68 (Jon Bing & Olav Torvand eds., 1995).

[89] Colin J. Bennett, REGULATING PRIVACY 101 (1992).

[90] *Id.* at 101-11.

[91] *Bundesdatenschutzgesetz* Dec. 1990, 20 *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes*, as amended.

[92] Cunningham, *supra* note 81, at 653.

[93] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, 108 E.T.S. 1 (entered into force Oct. 1, 1985).

[94] Cunningham, *supra* note 81, at 653.

[95] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EU).

[96] *Id.* at 38.

[97] *Id.*

means of the processing of personal data."[98] The Directive authorizes personal data processing only if certain conditions occur. There are heightened protections afforded to special categories of personal information including, "race or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life."[99] A judicial remedy addresses breach of the national provisions adopted pursuant to this Directive.[100] The adoption of the TFEU in 2012, which states that "everyone has the right to the protection of personal data concerning them," reinforced this right.[101]

C. Recent Developments in EU Data Protection Policy

In 2012, the European Commission decided that the Directive was no longer current[102] and there were gaps in the protection of individuals' personal data because of rapid technological advances that had taken place.[103] The proposed General Data Protection Regulation (GDPR),[104] which took effect in May of 2018, is Europe's proposal to upgrade the principles of the Directive so as to be most effective in the new digital age.[105] The stipulated goals for the GDPR are: (i) to address the impact of new technologies; (ii) to enhance the internal market dimension of data protection; (iii) to address globalization and improve international data transfers; (iv) to provide a stronger institutional arrangement for the effective enforcement of data protection rules; and (v) to improve the coherence of the data protection legal framework.[106]

The GDPR requires organizations to implement certain technical and organizational measures in order to secure data subject's rights and ensure

---

[98] *Id.*

[99] *Id.* at 40.

[100] *Id.* at 45.

[101] TFEU art. 16.

[102] *Protection of Personal Data*, EUR. COMMISSION, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en.

[103] Beata A. Safari, Comment, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 Seton Hall L. Rev. 809, 811 (2017).

[104] 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[105] European Commission Press Release IP/12/46, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), http://ec.europa.eu/rapid/press-release_IP-15-6321_en.htm.

[106] *See generally Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 7, COM (2010) 609 final (Nov. 4, 2010).

the proper processing of personal data.[107] It also specifically grants individuals the right to data portability, which is an additional challenge for companies holding and processing personal information.[108] Criticisms about the GDPR include it being overly complicated, that the language involves too much legalese, and that it does not lay out clearly enough the parameters and methods for achieving its stated goals.[109]

GDPR introduces a penalty system with significant fines, representing a significant change for businesses with connections to the EU. Article 83 of the GDPR provides for two levels of administrative fines for violations of certain provisions of the law including obligations of the data processor and controller, certification body, and monitoring body.[110] Infringements of any of these obligations can lead to administrative fines of up to €10,000,000 or 2% of a company's total worldwide annual turnover, whichever is higher.[111] More serious infractions under the law, including violation of a subject's data rights, violation of basic principles for processing such as conditions for consent, or unlawful transfers of personal data to third parties or international organizations, carry even heavier fines – up to €20,000,000 or 4% of a company's total worldwide annual turnover, whichever is higher.[112] For large companies handling a huge amount of data, such as Facebook and Google, these administrative fines under the GDPR could be enormous, and are likely to be the highest in the history of regulation.

Competition and data protection have very different origins, but in the EU especially, they are currently very dynamic areas of the law. Since 2007, competition enforcement actions in the EU, based on legal principles dating back to the Treaty of Rome, have become much more commonplace. Data protection law, on the other hand, has developed and gone through multiple changes since its introduction in 1995. With the introduction of GDPR, both bodies of law wield a great amount of power over companies that have a presence in the EU, giving the EU the power to levy high enough fines that they could hypothetically force violators to remedy their behavior.

IV. THE 2006 *ASNEF-EQUIFAX* CASE

In 2006, the Asociación de Usuarios de Servicios Bancarios (Ausbanc) sued the Spanish consumer credit reference agency Asnef-Equifax and the credit bureau registration Asnef-Equifax administered for violation of Article 81 of the EC.[113] Asnef-Equifax's credit bureau registration was intended to

[107] Lee A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 OSLO L. REV. 105, 106 (2017).

[108] GDPR, *supra* note 104, at art. 20.

[109] Bygrave, *supra* note 107, at 119.

[110] GDPR, *supra* note 104, at art. 83.

[111] *Id.* at art. 83(4).

[112] *Id.* at art. 83(5).

[113] Asnef-Equifax, *supra* note 1, at I-11149-50.

"provide solvency and credit information through the computerized processing of data"[114] which included information related to "the identity and economic activity of debtors."[115] This sort of information sharing is commonplace in the credit reporting industry as it allows for a mutually beneficial business model for consumers, lenders, and the economy.[116]

Case-law on information exchange agreements indicates that such agreements violate competition law only if they reduce or remove uncertainty in market operations so as to restrict competition.[117] The court agreed with Asnef-Equifax and held that the horizontal information sharing was harmless, arguing that the arrangement would likely "improv[e] the functioning of the supply of credit"[118] and increase the mobility of consumer credit.[119] Whether the proposed consumer benefit has actually manifested since this decision is unclear, though the global financial crisis would seem to indicate that it has not.[120] Most significantly for the topic of this note, the court held that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law"[121] and "may be resolved on the basis of the relevant provisions governing data protection."[122]

There are a few plausible reasons for the court's decision. First, integration of EU credit markets was at the time a top priority for the EU at the time and helped facilitate the four freedoms – free movement of goods, capital, services, and people[123] - of the European market.[124] Second, there was little substantive overlap and sometimes even conflict between the two bodies of law.[125] Third, the court viewed data protection law in Europe as robust and thought that it should be left to function as intended. Though in 2006 these reasons may have held weight, what has transpired since makes

---

[114] *Id.* at I-11149.

[115] *Id.*

[116] *See* Rothemund & Gerhardt, *supra* note 14; *see also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Single Market Act: Twelve Levers to Boost Growth and Strengthen Confidence*, at 3, COM (2011) 206 final (Apr. 13, 2011) [hereinafter *Commission Communication*].

[117] Asnef-Equifax, *supra* note 1, at I-11160.

[118] *Id.* at I-11160.

[119] *Id.* at I-11162.

[120] Federico Ferretti, *The Legal Framework of Consumer Credit Bureaus and Credit Scoring in the European Union: Pitfalls and Challenges - Overindebtedness, Responsible Lending, Market Integration, and Fundamental Rights*, 46 SUFFOLK U. L. REV. 791, 791 (2013).

[121] Asnef-Equifax, *supra* note 1, at I-11164.

[122] *Id.*

[123] *Commission Communication*, *supra* note 116.

[124] Ferretti, *supra* note 120, at 791.

[125] *Id.* at 821. Compliance with the Directive's requirements for notice to data subjects regarding the type and amount of personal information held by credit reporting companies took the back seat to competition concerns.

the court's reasoning less convincing.

The global financial crisis of 2008, which hurt many consumers, occurred at least partially because lenders were granting loans to consumers who could not afford them, something information sharing by credit reporting agencies was meant to prevent.[126] Hacking attacks have proliferated[127] and companies making money by controlling and using personal and private data have amassed enormous market power.[128] It is far from clear that the comprehensive yet reactive GDPR will be sufficient to protect consumer interests.

Despite the flaws in the *Asnef-Equifax v. Ausbanc* ruling, the court has held in a similar fashion in subsequent cases. In 2010, the ECJ held in *AstraZeneca v. Commission* that to bring a competition case on the basis of an abuse of dominant market position, there must be "at the very least evidence that . . . [the] conduct is such as to restrict competition,"[129] effectively excluding causes of action based on privacy concerns.[130] The European Commission cleared the Facebook/WhatsApp merger in 2014 because data concentration was not seen to create competitive concerns.[131] However, the 2016 review of that case and new investigation by German competition authorities may indicate a new willingness from EU authorities to change their approach when it comes to data protection and competition.[132]

A change, sooner rather than later, would be well advised as consumer information becomes more vulnerable and valuable to hackers. In 2011, a FBI chief cyber official warned of the increasing frequency and severity of cyber-attacks, and this is exactly what the world has witnessed since.[133] In 2017, credit agency Equifax suffered a data breach involving the sensitive personal information of 143 million people, and globally, nearly two billion total records have been lost or stolen in the first half of the year.[134]

Hackers are also increasingly sophisticated in the type of data they

---

[126] *See id.* at 823. *See generally* KATHLEEN C. ENGEL & PATRICIA A. MCCOY, THE SUBPRIME VIRUS: RECKLESS CREDIT, REGULATORY FAILURE, AND NEXT STEPS (2011).

[127] Cunningham, *supra* note 81, at 645.

[128] *Regulating the Internet Giants: The World's Most Valuable Resource No Longer Oil, but Data*, ECONOMIST, May 6, 2017, at 1, ProQuest, ID. 1895941741. Alphabet (Google), Amazon, Apple, Facebook, and Microsoft collectively made $25 billion in net profit in the first quarter of 2017.

[129] Case T-321/05, AstraZeneca v. Comm'n, 2010 E.C.R. II-2830, II-3151-52.

[130] Giovanni Buttarelli, *Strange Bedfellows: Data Protection, Privacy and Competition*, 34 COMPUTER & INTERNET LAW. no. 12, 2017, at 1, 2.

[131] Commission Decision in Case COMP/M.7217 at ¶ 164.

[132] Boot & Petropoulos, *supra* note 64.

[133] *See* Cunningham, *supra* note 81, at 672; Gerry Smith, *Cyber-Crimes Pose 'Existential' Threat, FBI* Warns, HUFFINGTON POST (Jan. 12, 2012, 2:26 PM), http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html.

[134] Selena Larson, *Why Hacks Like Equifax Will Keep Happening*, CNN (Sept. 29, 2017, 8:49 AM), http://money.cnn.com/2017/09/29/technology/business/equifax-hack-2017-cyberattacks/index.html.

target, going after the most sensitive consumer information such as medical records and social security numbers.[135] In response, the EU must take steps to better protect consumers and their fundamental right to privacy.[136] A new method of authentication, biometrics - proposed for use by airports and financial institutions and implemented on the iPhone - poses an even greater risk for consumers, since biometric information is even less replaceable than a social security number.[137] Such technological advances for the purposes of supposedly increased security and convenience make it even more important to implement strong policies to protect consumer data.

V. ACTIONS THAT EU CAN TAKE

In response to the increased security threat to consumer data, there are a few different routes the EU can pursue. First, the EU can continue to treat competition law and data protection law as independent bodies of law, consistent with the *Asnef-Equifax* decision. Second, the EU can develop a new body of law to cover the grey area where competition law and data protection overlap and conflict. Finally, the EU can choose to apply existing law differently, namely Article 101(3) of the TFEU, so that consumer welfare is considered during merger review and competition lawsuits like *Asnef-Equifax*.

A. Separate Treatment of Competition and Data Protection Law

The first option is viable, if not ideal, because of the lengths the EU took to ramp up and strengthen its data protection law in the last five years. The EU announced its decision to draft a new regulation that would replace the 1995 Directive in 2012,[138] and the GDPR finally became binding and applicable on May 25, 2018.[139] The independent development of data protection law makes it somewhat similar to sector regulation. There is a history of various industries, including telecommunications, water services, electricity, and aviation, adopting sectoral regulation because those particular industries were exempt from following the standard rules of competition.[140]

---

[135] Federico Ferretti, *The Consumer Interest and Data Protection Under EU Competition Law: The Case of the Retail Financial Services Sector*, 22 EUR. REV. PRIV. L. 485, 510 (2014).

[136] *Id.* at 506.

[137] Michael Corkery, *Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead*, N.Y. TIMES (Jun. 21, 2016), https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html?_r=0.

[138] EUROPEAN COMMISSION, *supra* note 102.

[139] W. Scott Blackmer, *GDPR: Getting Ready for the New EU General Data Protection Regulation*, INFOLAWGROUP LLP (May 5, 2016), https://www.infolawgroup.com/blog/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation?rq=W.%20Scott%20Blackmer.

[140] Maher M. Dabbah, *The Relationship Between Competition Authorities and Sector*

Sectoral regulation is typically broader in scope than competition law, going beyond economic considerations to impose technical and access requirements.[141] Likewise, the GDPR covers more ground in the data privacy and protection space than EU competition law would or could. Traditional sectoral regulation and data protection regulation diverge when the law operates: sectoral regulation tends to be proactive, whereas data protection regulation is reactive.[142] This means that it is unlikely the data regulation will come into play without some sort of data breach event, making it very likely that consumers will suffer some sort of harm. Despite being the easiest route for the EU, the threat of increasing consumer harm means the status quo——the do-nothing approach——is not optimal.

B. Creation of a New Body of Law

The EU also has the option of drafting an entirely new body of law to cover the current gap and the occasional conflict between competition law and data protection law. As already discussed, however, the drafting and procedural process for enacting new regulatory law is very slow.[143] With the increasing threat of hack attacks, unnecessary delay will be harmful to consumers and not optimal. Further, many companies, especially technology companies that process large amounts of data, have expended time, energy, and resources to understanding and readying for compliance under GDPR.[144] These companies would not be happy about having to comply with an additional, complicated body of law.[145] Therefore, this option is the least viable because it involves the largest amount of government work, would not offer adequate protection to consumers within the relevant timeframe, and would exacerbate companies' frustrations with the already complicated EU regulation requirements.

C. New Application of Existing Laws

The third path available to the EU is changing how to apply existing competition law and integrating certain data protection concepts into the competitive review process. This route, while requiring some work from the EU, would increase the safeguards on individual data and could even help companies proactively strengthen their internal data protection systems and comply with GDPR, before a breach arises. The European Data Protection

Regulators, 70 CAMBRIDGE L. J. 113, 113 n.1 (2011).

[141] *Id.* at 114-15.

[142] *See id*. at 115.

[143] *See* Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479, 479 (2016).

[144] Aliya Ram, *Tech Sector Struggles to Prepare for New EU Data Protection Laws*, FINANCIAL TIMES (Aug. 29, 2017), https://www.ft.com/content/5365c1fa-8369-11e7-94e2-c5b903247afd.

[145] Burri & Schär, *supra* note 143, at 488.

Supervisor (EDPS) recommended as such, proposing that the Commission broaden the concept of consumer harm to include violation of individual data rights.[146] The hook for this approach would be Article 101(3) of the TFEU, which allows for an exception to certain competition violations, like an agreement to share information, if such behavior "contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit."[147]

During a 2015 speech, Competition Commissioner Margrethe Vestager stated that "sometimes, intellectual property rights can be used to restrict competition" which can "also harm consumers."[148] She concluded that in situations where intellectual property law does not fully promote consumer welfare, competition law can be used as a balancing complement.[149] One solution the EU can consider is the interaction between the FRAND patent standard and competition law.[150] A similar scheme can be established between competition law and data protection law; in situations where consumer welfare is not fully covered by data protection law, competition law could be used as a balancing complement. Two situations where this integrated approach could prove useful are (i) data exchange between companies[151] and (ii) the merging of companies holding large amounts of consumer data. This solution would be apt considering the similarities between the European rights-based data protection regime and intellectual property law.

D. Possible Avenues of Implementation

The first place where this complementary integration can occur is in the competition law process of merger review.[152] While going through the merger review process, the European Commission can incorporate a review of the amount of data held by the consolidating entities as well as a review of their respective privacy policies. The Commission has expressed concern that consolidation and market power allows newly merged companies to take data protection less seriously, thereby increasing the risk of harm to

---

[146] Francisco Costa-Cabral, *The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law*, 23 Maastricht J. EUR. & COMP. L. 495 (2016).

[147] TFEU art. 101(3).

[148] Margrethe Vestager, Comm'r, European Comm'n, 19th IBA Competition Conference: Intellectual Property and Competition (Sep. 11, 2015).

[149] *Id.*

[150] Benjamin C. Li, *Patent Law: The Global Convergence of FRAND Licensing Practices: Towards "Interoperable" Legal Standards*, 31 BERKELEY TECH. L.J. 429 (2016).

[151] *See* Matthew Rosenberg, Nicolas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N. Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[152] *See* Darren S. Tucker, *The Proper Role of Privacy in Merger Review*, CPI ANTITRUST CHRONICLE 2 (May 2015).

consumers.[153]

Like the conditional grant of approval made by the Commission in Microsoft's acquisition of LinkedIn, the Commission could make merger clearance conditional on companies having a robust, post-acquisition GDPR compliant data protection policy. Incorporating data protection principles into merger review would lead to stronger protection of consumer information while giving large companies the opportunity to be proactive in ensuring a post-close GDPR compliant data protection policy. This approach would be particularly favorable for companies if the company can use the post-close GDPR compliance as a defense, and therefore a way to avoid the severe penalties, should the company experience a data breach in the future.

Competition law violation suits provide a vehicle to integrate data protection and competition law.[154] In contrast to the decision made by the ECJ in 2006, through Article 101(3)of the TFEU[155] the Court could find that horizontal data sharing is anti-competitive, by failing to provide the consumer with a fair share of the benefits, unless the data protection policy is strong enough to adequately protect the consumer data being shared. In the current age of information, where serious hack attacks are happening more frequently, a lack of robust and GDPR compliant data protection policies at all the businesses involved in sharing consumer information will likely lead to significant consumer harm and few benefits. Adding in data protection policy requirements would add a layer of protection for consumers and businesses, making horizontal information sharing more likely to create mutual benefits.

As discussed above, consumers and businesses both stand to gain from integrating certain data protection concepts into the competition law processes of merger review and violation suits.[156] Additionally the government would stand to gain under such a policy. First, consumers will benefit because their personal data and information will enjoy better protection. Businesses will benefit because having their data protection policies placed under review, especially during the merger review process but also during competition suits like *Asnef-Equifax*, could help them avoid steep GDPR administrative fines[157] later. The government would also likely benefit because they would not have to create any new laws to fill the current gap between competition law and data protection. The caseload for data protection violations would also likely decrease because of the proactive

---

[153] Commission Decision in Case COMP/M.8124 at ¶ 350.

[154] Inge Graef, Big Data in the Platform Economy Conference: Data Aggregation in the Competition Law Analysis (May 13, 2016) (unpublished presentation)(on file with Lirias), https://lirias.kuleuven.be/bitstream/123456789/541423/2//Big+data+in+the+platform+economy+-+Data+aggregation+IGraef.pdf.

[155] TFEU art. 101(3).

[156] Max Huffman, *Bridging the Divide? Theories for Integrating Competition Law and Consumer Protection*, 6 EUR. COMPETITION J. 7, 8 (Apr. 2010).

[157] *See generally* GDPR, *supra* note 104, at art. 83(4)-(5).

prevention of violations. If the goal of the government is to incentivize strong internal data protection policies for the benefit of consumers, this path is more sensible compared to the other options.

This would not be the case, however, if the reason for GDPR and the recent antitrust suits was simply to make money by levying steep fines. It is interesting to note that nearly all of the companies that have been subject to merger review scrutiny, competition suits, and possible penalties have been U.S. companies, and none have been headquartered in the EU.[158] Recently Qualcomm, a U.S. company that manufactures computer chips, was slapped with a € 997,439,000 fine (approximately $1.2 billion in U.S. dollars) for EU antitrust violations.[159] That U.S. high-tech companies have faced the brunt of the EC's antitrust scrutiny has been viewed as self-serving and protectionist.[160] According to a new empirical study on European Commission merger control between 1990 and 2014, the data does not appear to support the hypothesis that enforcement in the EU is motivated by protectionism.[161]

One possible drawback to the implementation of an integrated data protection and competition law approach is that it might increase scrutiny concerning data protection on new market entrants. These companies would be less likely than their larger competitors to have the resources and expertise necessary to implement robust internal data protection policies. These high expectations and regulatory hurdles could therefore lessen competition by discouraging new market entrants who would have otherwise entered in a less strict regulatory environment. Independently, GDPR will likely have a similar effect which means this concern should not be a reason not to use the integrated approach. In fact, looking forward, the implementation of the integrated approach would allow the EU to get ahead on protection of even more valuable consumer data before it hits the mass market. Such data will include biometric data (fingerprint, retina scan, etc.), electronic medical files, and DNA profile data, and will likely be widely collected and used by companies in the near future, to pass through airport security and perhaps even to make payments.[162]

---

[158] Of the cases discussed in this note which have been brought against companies by the ECJ, only Samsung is a non-U.S. company. It is a South Korean company headquartered in Seoul.

[159] European Commission Press Release IP/18/421, Antitrust: Commission Fines Qualcomm €997 Million for Abuse of Dominant Market Position (Jan. 24, 2018), http://europa.eu/rapid/press-release_IP-18-421_en.htm.

[160] Mark Scott, *Antitrust and Other Inquiries in Europe Target U.S. Tech Giants*, N. Y. TIMES (Apr. 2, 2015), https://www.nytimes.com/2015/04/03/technology/europe-regulators-apple-google-facebook.html.

[161] Anu Bradford, Robert J. Jackson & Jonathon Zytnick, *Is EU Merger Control Used for Protectionism? An Empirical Analysis*, 15 J. EMPIRICAL LEGAL STUD. 165, 165 (2018).

[162] Claire Martin, *Passing Through Airport Security with the Touch of a Finger*, N. Y. TIMES (Sept. 8, 2017), https://www.nytimes.com/2017/09/08/business/airport-security.html.

VI. CONCLUSION

In conclusion, the best course of action for the EU is to implement an approach to competition law which incorporates certain data protection concepts. This integrated approach would serve as a complement to the already existing and robust bodies of competition and data protection law in the EU, and would provide another layer of protection for both consumers and companies. If implemented correctly it could lessen the risk of harm of data breach events to consumers, and lessen the risk of penalties faced by large companies controlling large amounts of vulnerable consumer data.

The integrated approach is optimal because of its relatively low cost to implement, while offering significant gains to all interested parties: the consumers, the business community, and the government. The main point of contact between businesses and the government where this approach can be put to use is during the process of merger review. Additionally, the courts would have the option of reviewing and taking into consideration the data protection policies of companies subject to review as a result of anti-competitive challenges, as was the case with *Asnef-Equifax*.

European efforts to strengthen data protection law through the implementation of GDPR, and their increased enforcement of competition law against big technology companies indicate that Europe is ready for the added benefits of this integration. Things are very different in the U.S., however, and currently it seems unlikely that the integrated approach would be transferrable to the U.S.[163] The first step for the United States will be developing a uniform data protection law, like the EU's 1995 Directive or the 2018 GDPR. Until then, the integration of competition law and data protection law will remain a European creation.

[163] P.J. Harbour, *The Transatlantic Perspective: Data Protection and Competition Law*, *in* DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? (Hielke Hijmans & Peter Hustinx eds., 2014).