Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 30 *XXX*
Number 1

Article 4

2019

Towards a Transatlantic Concept of Data Privacy

Erdem Büyüksagis
Antalya Bilim University, erdem.buyuksagis@antalya.edu

Towards a Transatlantic Concept of Data Privacy

Cover Page Footnote

Full Professor of Law, Antalya Bilim University; Professor of Law, University of Fribourg. While writing this paper, I have been fortunate to benefit from a Fulbright grant, for which I am thankful. I owe a debt of gratitude to Professor Deborah Hensler for inviting me as a Fulbright Visiting Professor to Stanford Law School for a productive one-year sabbatical during the 2018–2019 academic period. The opportunities she provided throughout my stay at Stanford have meant a lot to me. I also thank Professor Dorothy Glancy of Santa Clara University Law School for her generous and insightful comments on a draft of this paper. Finally, I would like to thank Marta Infantino, Assistant Professor at the University of Trieste, for her help with the Italian sources, and Lotte Meurkens, Assistant Professor at Maastricht University, for her help with the Dutch sources.

Towards a Transatlantic Concept of Data Privacy

Erdem Büyüksagis*

Due to ever-growing big data and the ease with which information can be transmitted over the Internet, it has become more complicated for individuals to enjoy their rights to access, to rectify and erase personal information, and for the judiciary to apply conventional privacy law rules, such as consent, transparency, and purpose limitation. On both sides of the Atlantic, this phenomenon has motivated legislatures and courts to extend protective measures in data privacy. Nevertheless, data protection standards in the United States and the European Union ("EU") appear to many observers to be radically different and even mutually incompatible. The European Court of Justice's ruling in Google Spain *led many to assume that EU law gives more importance to data protection than does U.S. law.*

In this Article, I argue that the United States and the EU do in fact give similar levels of legal and regulatory protection to private data. Despite the Google Spain *decision, the absence of an explicit reference to privacy or data protection in the U.S. Constitution, and cultural differences regarding the value placed on privacy between these jurisdictions, critics have not offered any convincing argu-*

* Full Professor of Law, Antalya Bilim University; Professor of Law, University of Fribourg. While writing this paper, I have been fortunate to benefit from a Fulbright grant, for which I am thankful. I owe a debt of gratitude to Professor Deborah Hensler for inviting me as a Fulbright Visiting Professor to Stanford Law School for a productive one-year sabbatical during the 2018–2019 academic period. The opportunities she provided throughout my stay at Stanford have meant a lot to me. I also thank Professor Dorothy Glancy of Santa Clara University Law School for her generous and insightful comments on a draft of this paper. Finally, I would like to thank Marta Infantino, Assistant Professor at the University of Trieste, for her help with the Italian sources, and Lotte Meurkens, Assistant Professor at Maastricht University, for her help with the Dutch sources.

ments to show that either the perception of privacy or the consequences of its violation are radically different in the United States and in Europe. First, when assessing whether private data gathered by governments agencies or private businesses ought to be made available to the general public, courts in both jurisdictions take into account the nature of the information in question, its sensitivity for the data subject's privacy, the data subject's identity, the reasons behind the storage and disclosure of the information, and the public's interest in the information. My point is illustrated by the fact that courts in the United States and the EU rely upon similar tests to deal with potential data breaches. Second, particularly since the adoption of the General Data Protection Regulation, data protection is on the agenda of a number of state legislatures in the United States. The adoption of the California Consumer Privacy Act constitutes a non-negligible shift in the nation's data privacy regime, since its effective territorial reach will not be limited to California, but will involve all the states given as the headquarters of hundreds of high technology companies that are based in the region commonly known as "Silicon Valley."

My analysis leads me to the conclusion that the regulatory and case law developments on both sides of the Atlantic hint at a harmonization process of data protection standards because of the ever-growing recognition of the need for specific data protection laws and their substantive convergence.

INTRODUCTION

In Oscar Wilde's play "An Ideal Husband," one of its characters, Mrs. Cheveley, asserts that no man is "rich enough . . . to buy back [his] past."[1] Wilde's idea has continuing validity in our digital age, where information technology compresses time into a "perpetual"[2] present and creates a "digital panopticon."[3] This phenomenon, which puts private life no more than a few keystrokes away from

---

[1] OSCAR WILDE, AN IDEAL HUSBAND act 1, at 46 (The Floating Press 2008) (1895).

[2] Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 416 (2015).

[3] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 197 (2009) (referring to Bentham's panopticon). A panopticon permits a watchman to watch occupants without the occupants knowing whether or not they are being observed. *See The Panopticon*, U.C. LONDON, https://www.ucl.ac.uk/bentham-project/who-was-jeremy-bentham/panopticon [https://perma.cc/26QQ-7GCE].

anyone connected to the global Internet, unavoidably shrinks the respect data controllers[4] have for data subjects' autonomy.[5]

Data privacy issues arise, in general, from a mass violation of data subjects' autonomy.[6] Reflecting the large scale of this violation, litigation of this issue in the United States has tended to take the form of class-action lawsuits. The class-action lawsuits filed against

---

[4] According to the OECD Privacy Guidelines, a "data controller" is defined as the "party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf." ORG. FOR ECON. CO-OPERATION AND DEV., THE OECD PRIVACY FRAMEWORK 13 (2013), www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/86TW-A83G].

[5] According to the OECD Privacy Guidelines, a "data subject" is the natural person who is identified, or can be identified, by reference to her or his personal data. *Id.*

[6] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 58 (2003) (discussing "holes in this patchwork of sector-specific privacy laws"). For a comparison with EU law, see PAUL B. LAMBERT, UNDERSTANDING THE NEW EUROPEAN DATA PROTECTION RULES 12 (2018) (arguing that the "issue-by-issue approach . . . leaves many gaps and areas not covered by data protection in the United States"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014) (asserting that "[c]omparisons between privacy regulation in the United States and European Union have often pointed out E.U. law's comprehensiveness in contrast with U.S. law's fragmentation and hollow standards, which provide few limits on the collection, use, and disclosure of personal data").

Facebook,[7] Equifax,[8] Target,[9] Yahoo!,[10] Home Depot,[11] Sony Pictures,[12] Anthem,[13] and Ashley Madison[14] illustrate the problem of

---

[7] In March 2018, Facebook declared that the personal data of 87 million users worldwide had been collected through an app from November 2013 to May 2015 and transferred to Cambridge Analytica, a political consulting firm. Millions of users' data was accessed and exploited, without the data subjects' consent, to create politically useful profiling and micro-target citizens, giving campaign groups the ability to connect with individual voters. In January 2019, a complaint was filed with the Federal Trade Commission accusing Facebook of misleading practices. The plaintiffs alleged that personal health information about positive HIV diagnoses, sexual histories, details of past sexual abuse, substance abuse disorders, and a wide range of health and mental health conditions disclosed by users of closed Facebook groups had been made public. Sarah Tejares, *FTC Accuses Facebook of Revealing Sensitive Health Data in Group*, MED. DAILY (Feb. 19, 2019, 5:42 AM), www.medicaldaily.com/ftc-accuses-facebook-revealing-sensitive-health-data-group-429927 [https://perma.cc/U4H9-E5XK].

[8] Equifax, one of the nation's largest credit reporting companies, has recently revealed a massive data breach that affected more than 148 million Americans. In its statements made in 2017 and 2018, the company reported that the names and dates of birth of approximately 147 million people were exposed, as well as 145.5 million Social Security numbers, the address information for 99 million people, the gender data for 27.3 million people, 20.3 million consumers' phone numbers, 17.6 million driver's license numbers, 1.8 million email addresses, 209,000 credit card numbers and expiration dates, and 97,500 tax ID numbers. *See* Press Release, Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/G9B6-7E8Z]. *See also* Thomas Brewster, *Equifax Just Got Fined up to $700 Million for That Massive 2017 Hack*, FORBES (July 22, 2019), www.forbes.com/sites/thomasbrewster/2019/07/22/equifax-just-got-fined-up-to-700-million-for-that-massive-2017-hack/#4c96c33c3e96 [https://perma.cc/LRU3-PBQX].

[9] Target failed to identify a subcontractor's lax security and was thus the victim of a sophisticated hacking attack that resulted in 40 million customers' debit and credit cards being exposed and 70 million customers' nonfinancial personal information being stolen. *See* Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html [https://perma.cc/C2EG-VY5W]; Jonathan Stempel & Nandita Bose, *Target in $39.4 Million Settlement with Banks over Data Breach*, REUTERS (Dec. 2, 2015), www.reuters.com/article/us-targetbreach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203 [https://perma.cc/G5RM-7CXW].

[10] In September 2016, Yahoo confirmed that it had experienced a huge data breach in late 2014 in which 500 million users' PII, encrypted passwords, and in some cases security questions were hacked by a "state-sponsored actor." Three months later, the company revealed another and even more important hack resulting in the data of over 1 billion users being compromised in August 2013. *See* Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), www.nytimes.com/2016/09/23/technology/yahoo-hackers.html; [https://perma.cc/QED3-P8UB]; Vindu Goel & Nicole

data privacy protection, and explain why most people think that their personal privacy may gradually come to an end unless corrective

Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/38J6-G2CQ].

[11] In 2014, hackers used malware that infected the Home Depot payment systems and compromised 56 million customers. The hackers reportedly remained in the company's computers, unnoticed, for about five months. *See* Melvin Blackman, *Home Depot: 56 Million Cards Exposed in Breach*, CNN (Sept. 18, 2014), http://money.cnn.com/2014/09/18/technology/security/home-depot-hack [https://perma.cc/FKZ7-NNRW]; Jonathan Stempel, *Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016), www.reuters.com/article/us-home-depot-breachsettlement-idUSKCN0WA24Z [https://perma.cc/9RDF-TQUK].

[12] In 2014, entertainment company Sony experienced an extensive data breach that disclosed a huge amount of intellectual property and sensitive personal information. In the days following the public disclosure of the breach, the hackers started leaking yet-unreleased films, unfinished manuscripts and eight portions of the estimated twenty-five gigabytes of sensitive or confidential data they had stolen. *See* David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html [https://perma.cc/PE8H-2CYJ]; Jody Godoy, *Sony to Pay up to $4.5M to Settle Employee's Breach Suit*, LAW360 (Oct. 20, 2015), www.law360.com/articles/716417/sony-to-pay-up-to-4-5m-to-settle employees-breach-suit [https://perma.cc/L9VN-NTWR] .

[13] Several massive hacks have been directed at the healthcare sector, a trend that is likely to go on given the high value of personal medical information. In 2015, for instance, close to 80 million personal records were stolen from Anthem, a large medical insurance company, as a result of questionable internal storage. *See* Joseph Conn, *Legal Liabilities in Recent Data Breach Extend Far Beyond Anthem*, MOD. HEALTHCARE (Feb. 23, 2015), https://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem [https://perma.cc/4848-EDHA]; Bruce Japsen, *Hackers Stole Data on 80 Million Anthem Customers. Why Wasn't It Encrypted?*, FORBES (Feb. 6, 2015), https://www.forbes.com/sites/brucejapsen/2015/02/06/anthem-didnt-encrypt-personal-data-and-privacy-laws-dont-require-it/#bdff22d4593e [https://perma.cc/YE54-WXLT].

[14] An anonymous hacker group calling itself "The Impact Team" hacked into the online cheating website and menaced to release the stolen information unless the owners permanently shut down the site. As the website owners refused, the hackers uploaded around thirty gigabytes of stolen data onto the dark web, thus exposing the personal account information of the site's users, as well as data about the company and its employees. *See* Chris Baraniuk, *Ashley Madison: 'Suicides' over Website Hack*, BBC (Aug. 24, 2015), www.bbc.com/news/technology-34044506 [https://perma.cc/ZPJ9-FP7K]; Brian Krebs, *Online Cheating Site Ashley Madison Hacked,* KREBS ON SECURITY (July 15, 2015), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked [https://perma.cc/34TU-BC82]; Kim Zetter, *Ashley Madison Hackers Release an Even Bigger Batch of Data*, WIRED (Aug. 20, 2015, 3:01 PM), https://www.wired.com/2015/08/ashley-madison-hackers-release-even-bigger-batch-data/ [https://perma.cc/6A5P-9KVY].

actions are taken. Some individual[15] as well as class actions[16] brought against Google on privacy and data security related issues in the European Union ("EU") reflect similar concerns regarding data consent policies that do not give users enough control over the way their information is collected and processed.

The growing concern has prompted lawmakers on both sides of the Atlantic to introduce new laws and proposals to address threats to privacy and data security. The EU legislature replaced the 1995 Data Protection Directive with the General Data Protection Regulation ("GDPR"),[17] and unified data protection within the EU.[18] Article 3 of the GDPR reads that the Regulation applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the [European] Union, regardless of whether the processing takes place in the [European] Union or not."[19] This centralized approach significantly lessened the burden on information technology businesses, since they no longer have to comply with the various sensitivities of each EU member state.[20]

In the United States, some legislative efforts at the state level, like the newly adopted California Consumer Privacy Act ("CCPA"), aim at strengthening consumers' privacy rights in a limited geographical area,[21] whereas a diverse collection of different types

---

15 *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317.

16 Following the fine imposed by France's data watchdog on Google for failing to implement adequate measures to meet the requirements of the GDPR, in June 2019, a French consumer group filed a class-action against Google for improper collection of location tracking data. *See French Consumer Group Files Class-Action Against Google for Alleged GDPR Violations*, IAPP (June 27, 2019), https://iapp.org/news/a/french-consumer-group-files-class-action-against-google-for-alleged-gdpr-violations/ [https://perma.cc/6TS6-EPX7].

17 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].

18 LAMBERT, *supra* note 6, at 12.

19 GDPR, *supra* note 17, art. 3.

20 Lisa Owings, *The Right to Be Forgotten*, 9 AKRON INTELL. PROP. J. 45, 62 (2015).

21 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.198(a) (2018). For an analysis see Lydia de la Torre, *A Guide to the California Consumer Privacy Act of 2018*, SANTA CLARA U., https://ssrn.com/abstract=3275571 [https://perma.cc/8ZJ4-URCM]; Eric

of rules govern privacy and data protection at the national level.[22] Obviously, some sensibilities about privacy differ between the United States, with its solid free-speech tradition,[23] and Europe, with its painful experience of Nazi propaganda.[24] The different attitudes towards privacy lead, in turn, to diverse legislative schemes impacting the method of protection.[25] Although there have been some signs of change,[26] the data protection policy of the United States

---

Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, IAPP (July 9, 2018), https://iapp.org/media/pdf/resource_center/Intro_to_CCPA.pdf [https://perma.cc/VR8N-H9X3].

[22] On these rules, see Dorothy J. Glancy*, At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUT. & HIGH TECH. L.J. 357, 359 (2000); 37th Int'l Privacy Conference Amsterdam 2015, *Privacy Bridges*, EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS 16–17 (2015), https://privacybridges.mit.edu/sites/default/files/documents/Privacy Bridges-FINAL.pdf [https://perma.cc/4UPA-JLUP] [hereinafter *Privacy Bridges*]; Cameron F. Kerry, *Filling the Gaps in US Data Privacy Laws*, BROOKINGS INST. (July 12, 2018), www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws [https://perma.cc/9XCM-BYHC]. It is worth noting that a number of state constitutions, namely those of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington, expressly provide for a right to information privacy. *See Privacy Protections in State Constitutions*, NAT'L CONF. ST. LEGISLATURES (Nov. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/N3H5-9R7Q].

[23] Glancy, *supra* note 22, at 355–66; Jean-Marie Kamatali, *The Limits of the First Amendment: Protecting American Citizens' Free Speech in the Era of the Internet & the Global Marketplace of Ideas*, 33 WIS. INT'L L.J. 101, 130 (2016).

[24] Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 423 (2002); *see also* JACQUELINE KLOSEK, THE WAR ON PRIVACY 78 (2007) (noting that "[i]n the years following World War II, in light of the horrors raised by the holocaust, governments were sensitive to the importance of respecting their citizens' right to maintain the privacy of certain personal information"); Michael W. Heydrich, *A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407, 417 (1999).

[25] *See* James Q. Whitman, *The Two Western Cultures of Privacy, Dignity Versus Liberty*, 113(6) YALE L.J. 1151, 1155 (2004) (The author argues that "[t]o the Europeans . . . it often seems obvious that Americans do not understand the imperative demands of privacy at all." He thinks that "[t]he Monica Lewinsky investigation, in particular, with its numerous and lewd disclosures, led many Europeans to that conclusion.").

[26] *See infra* Part III.A.

remains market-dominated, whereas the EU prefers a rights-dominated approach.[27]

On the basis of multiple *differences*, several commentators have noted that the United States and the EU have *conflicting* data protection standards.[28] The type of protection radically changes as data crosses the Atlantic. The obligations of the users and disseminators of data, both of which are primarily multinational corporations, change as well. The recent invalidation of the US–EU Safe Harbor Agreement,[29] which aimed at providing protection for the transfer of individuals' personal data from EU member states to organizations in the United States, might have contributed to creating that perception of conflict.[30] The landmark *Google Spain* decision handed down by the European Court of Justice ("ECJ")[31] in 2014 certainly reinforced the idea that EU law gives more importance to data protection than American law,[32] although EU law does have a

---

[27] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1318 (1999).

[28] *See, e.g.*, Leslie E. Minora, *U.S. Courts Should Not Let Europe's "Right to Be Forgotten" Force the World to Forget*, 89 TEMPLE L. REV. 609, 642 (2017) (arguing that "if and when a U.S. court faces [a right to be forgotten enforcement] decision, it should not enforce the right to be forgotten because it contravenes our First Amendment").

[29] Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 8.

[30] The US–EU Safe Harbor Agreement was heavily criticized in the United States. *See* David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 958 (2003) (arguing that "certification under Safe Harbor . . . face[s] strict constitutional challenges—for example, under the First Amendment principle of free flow of information").

[31] Case C-131/12*,* Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317.

[32] LEE C. BOLLINGER, THE TOLERANT SOCIETY: FREEDOM OF SPEECH AND EXTREMIST SPEECH IN AMERICA 7 (1986) (stating that "the free speech idea nonetheless remains one of our foremost cultural symbols"); Frederick Schauer, *First Amendment Opportunism*, *in* ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 175, 176 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002) (arguing that "different societies have different argumentative showstoppers, but in the United States it is often the First Amendment that serves this function"); Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 Harv. J.L. & Tech. 349, 416 (2015) (highlighting that "the difference in approaches to privacy rights can be attributed to America's unilateral protection of the freedoms of expression and the press under the First

doctrine that echoes the First Amendment right of freedom of expression.[33] Many describe the scrutiny levels applied to public disclosure of private facts in the United States and the EU as a "transatlantic clash."[34] Dean Post takes a step further and argues that *Google Spain* "forays into the significance of communication on the Internet."[35] According to another commentator, Professor Byrum, this situation has the potential of "unearth[ing] a myriad of global media law issues between the two continents."[36] A senior research fellow at Heritage Foundation adopts an extreme position and considers the GDPR a form of "imperialism" permitting the EU to aggressively assert jurisdiction over U.S. companies.[37]

Amendment and Europe's recognition of the countervailing right to private life in Article 8 of the ECHR"); Howard M. Wasserman, *Symbolic Counter-Speech*, 12 WM. & MARY BILL RTS. J. 367, 380 (2004) (describing the principle of freedom of speech as an "icon").

[33] Article 11 of the Charter of Fundamental Rights of the EU reads: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." Charter of Fundamental Rights of the European Union, art. 11(1), 2012 O.J. (C 326/391) 398.

[34] Franz Werro, *The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash*, *in* LIABILITY IN THE THIRD MILLENNIUM 285 (Aurelia Colombi Ciacchi et al. eds., 2009); *see also* Andrew Charlesworth, *Clash of the Data Titans? US and EU Data Privacy Regulation*, 6 EUR. PUB. L. 253 (2000); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976 (2013); Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, HARV. BUS. REV. (Apr. 9, 2018), https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain [https://perma.cc/2CZP-BN7B].

[35] See Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 1071 (2018).

[36] KRISTIE BYRUM, THE EUROPEAN RIGHT TO BE FORGOTTEN, THE FIRST AMENDMENT ENEMY xiii (2018); *see also* Jeffrey Rosen, *The Right to Be Forgotten*, ATLANTIC (July/Aug. 2012), www.theatlantic.com/magazine/archive/2012/07/the-right-to-be-forgotten/309044/ [https://perma. cc/RV4F-8WVC].

[37] Theodore Bromund, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*, HERITAGE FOUND. (Jan. 9, 2018), https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism [https://perma.cc/QEL3-MG25]. However, when it comes to the right to be forgotten, for instance, which is to be found in Article 17 of the GDPR, in its decision of September 24, 2019, the ECJ highlighted that "where a search engine operator grants a request for de-referencing . . . , that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the [EU] Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name

The analysis set forth in this Article shows that, despite the different values that American and European cultures attach to privacy, the United States and EU legal and regulatory regimes define data privacy in similar ways and impose similar consequences on those who violate data protections. First, any attempt at comparison between the American and EU systems based upon a generalization from just one case—as if these systems were monolithic and standalone—is inaccurate and simplistic. In the EU, even if *Google Spain* sets a milestone in the long-standing struggle to find a fair solution to data protection issues, it is not the only ECJ ruling that governs digital privacy. Likewise, "privacy" is not a fixed concept across all American jurisprudence, and American courts have developed a range of robust standards with which to assess different kinds of data privacy violations.[38] Professor Glancy rightly contradicts the beliefs of some[39] when, discussing data privacy law in the United States, she points out that "it [would be] a mistake to count privacy, and the laws which protect it, as zero."[40]

In parallel with global changes in the ways data is preserved and protected,[41] both the EU legislature and many American state legislatures have gained greater appreciation for the importance of data protection and have expanded the scope of data regulation. In fact, several states have already adopted, or are about to adopt, some of

---

from gaining access, via the list of results displayed following that search, to the links which are the subject of that request." *See* Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), 2019 E.C.R. 772, ¶ 73 (Sept. 24, 2019).

38 *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006).

39 While responding to a question at a product launch Scott McNealy (CEO of Sun Microsystems) said, "You have zero privacy. Get over it." *See* Michael Froomkin, *The Death of Privacy*?, 52 STAN. L. REV. 1461, 1463 (2000); Glancy, *supra* note 22, at 357 (2000) (both Froomkin and Glancy referring to what Scott McNealy said). McNealy's Sun Microsystems was a causality of the dot-com bubble.

40 Glancy, *supra* note 22, at 358.

41 According to the United Nations Conference on Trade and Development (UNCTAD), "107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy." *Data Protection and Privacy Legislation Worldwide,* UNITED NATIONS CONFERENCE ON TRADE & DEV., https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [https://perma.cc/48VL-YEQV]. *See also* Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY LAWS & BUS. INT'L REP. 10 (2017).

the protective measures found in the GDPR.[42] The CCPA, which gives consumers, among others, a right to request that a business delete any personal information that it has collected from its consumers,[43] or the legislative proposals recently introduced by a bipartisan group of lawmakers to adopt a strong, national privacy policy foretell the direction in which the protection of privacy and personal information is heading in the United States.[44]

The purpose of this study is neither to find a concept that could reconcile privacy with freedom of expression nor to provide a thorough description of data privacy laws in the United States and the EU. Rather, this study aims to demonstrate, from both practical and conceptual perspectives, that a multitude of variables influence any decision regarding a possible loss of privacy or restriction of freedom of expression. This Article will start by highlighting gaps in privacy and data protection at various levels, and these gaps' dramatic consequences for both individuals and businesses in the computerized world of the 21st century (II). This Article will then explain the dynamics of current legislative activities in the United States and the EU with reference to the debate on privacy in general and data protection in particular. This section of the Article will introduce the parallels between some factors driving the new privacy policy in both the United States and the EU, although the former sees privacy as in essence a civil right and the latter considers it to be a natural right (III).[45] This Article will then discuss the

---

[42] Rachel Marmor, Maryam Casbarro & Mike Khoury, *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT & TREMAINE LLP (Feb. 7, 2019) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou [https://perma.cc/4NTC-HWL3].

[43] *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.105(a) (2018) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

[44] *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 116th Cong. 2 (2019) (statement of Sen. Roger Wicker, Chairman, the S. Comm. on Commerce, Science and Transportation).

[45] Human rights are natural rights usually granted by the Constitution, held against the powers of the state, whereas civil rights are usually granted by state laws. This distinction is less important in Europe. For more information on this discussion, see Steven C. Bennett, *The "Right to Be Forgotten:" Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 168 (2012).

standards and tests that American and European courts respectively use to evaluate data protection (IV). Finally, this Article will indicate how such in-depth case-based study may be used not only to facilitate further legal analysis of the sprawling and complex notion of data protection, but also to show that courts on both sides of the Atlantic use fundamentally similar criteria to adjudicate data protection disputes.

I. NECESSITY OF MORE EFFECTIVE MEASURES

This section will discuss the necessity of more effective measures from the point of view of the protection of privacy in general and data protection in particular. I will first define what privacy means today, then focus on the methods that have been used to remedy privacy breaches or data misuse, and finally highlight the need, in an evolving technological landscape, for new ways of legal thinking.

A. Ineffectiveness of Existing Privacy Norms

The U.S. Constitution does not explicitly mention privacy or data protection, although the U.S. Supreme Court has found that the Constitution implicitly guarantees a fundamental right to privacy.[46] Privacy includes the protection of an individual's "private space."[47] As Garfinkel described in his book, Database Nation, "privacy [nevertheless] isn't just about hiding things. It's about self-possession, autonomy and integrity"[48] or, in the words of the Supreme Court, an "individual's control of information concerning his or her person."[49] This description is in line with Warren's and Brandeis' original thinking that the right to privacy was the right of each individual to

---

[46] Griswold v. Connecticut, 381 U.S. 479 (1965) (asserting for the first time an independent constitutional right of privacy, the Supreme Court held unconstitutional the Connecticut birth control statute prohibiting the use of contraceptives by married couples).

[47] *See Privacy Bridges*, *supra* note 22, at 12.

[48] SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 4–5 (2000).

[49] Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

determine, "ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[50]

The definition above reflects the traditional American conception of self-reliance, based on Emerson, Thoreau, Dickinson, and many other nineteenth century American writers.[51] Yet it is not very different form the European conception of privacy. Already in the seventeenth century, John Locke, one of the most influential European Enlightenment thinkers, had recognized the law of reputation is a necessary restraint to balance the desire for liberty.[52] Locke's insight influenced the notion of freedom proclaimed in Article 2 of the 1789 Declaration of the Rights of Man and the Citizen ("*Déclaration des droits de l'homme et du citoyen de 1789*"), which implicitly articulates respect for privacy.[53] The ECJ's analytical approach in *Google Spain* might be traced back to the French Revolution.[54]

Today, both the European Convention on Human Rights[55] and the Charter of Fundamental Rights[56] provide similar definitions to those found in court opinions in the United States. Article 8 of the Convention and similarly Article 7 of the Charter state that everyone has the right to respect for his or her private and family life, home, and communications. In *Evans*, the European Court of Human

---

50 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

51 Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 25 (1979) [hereinafter *Invention*].

52 JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING, *available at* https://www.globalgreyebooks.com/read-online/essay-concerning-human-understanding/read-online.html#_Toc530974960 [https://perma.cc/6RF4-7K9H] (1690). *See also* Michelle E. Brady, *Locke's Thoughts on Reputation*, 75 REV. POL. 335 (2013).

53 *See* Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62 (Fr.) (*affaire Rachel*) (the landmark Rachel decision handed down by the First Instance of Sarine Court, where the tort of privacy was first recognized in 1858). For the details of this case *see* Jeanne M. Hauch, *Protecting Private Facts in France: The Warren and Brandeis Tort Is Alive and Well and Flourishing in Paris*, 68 TUL. L. REV. 1219, 1233 (1994).

54 BYRUM, *supra* note 36, at xiv.

55 EUROPEAN COURT OF HUMAN RIGHTS COUNCIL OF EUROPE, EUROPEAN CONVENTION ON HUMAN RIGHTS (June 1, 2010), www.echr.coe.int/Documents/Convention_ENG.pdf. [https://perma.cc/5MRF-FUFJ] [hereinafter ECHR].

56 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326/393) 391.

Rights ("ECtHR") described, on the basis of Article 8 of the Convention, the "protect[tion] against interference with private life [as] an aspect of the principle of self-determination or personal autonomy."[57] The latter was described in a similar way by the California Supreme Court as an interest "in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference . . . ."[58] On both sides of the Atlantic, courts have adopted a wide-ranging interpretation of "private life."[59]

The right to digital self-determination or privacy is the logical reaction to countless privacy breaches,[60] and accordingly this right has become one of the most discussed and popular topics in the legal world.[61] When Warren and Brandeis published their paper on privacy in 1890, immigration was driving rapid population growth in the United States, with the result that life in many local communities was becoming less isolated and the cities were becoming more crowded.[62] In this context, personal privacy became much more difficult to attain or preserve.[63] Personal privacy was still in need of support and protection in 1970, when, under the theory of "captive audience," the Supreme Court in *Rowan* rejected a First Amendment challenge to a statute enabling people to refuse the Post Office permission to deliver mail from specific senders to their homes.[64] To-

---

57 Evans v. United Kingdom, App. No. 633/05, Eur. Ct. H.R. 1, 7 (2007).

58 Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994).

59 Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 276 (2014).

60 On the contemporary conception of privacy, see AMITAI ETZIONI, THE LIMITS OF PRIVACY 183 (1999). For an overview, see generally M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006). On the evolution of the right to privacy, see *Invention*, *supra* note 51.

61 Colin J. Bennett, *The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?*, 23 INFO. POLITY 239, 239 (2018) (saying that "[a]t no time in the past 40 years, has the protection of privacy been so prominently, globally and intensively debated").

62 OSCAR HANDLIN, IMMIGRATION AS A FACTOR IN AMERICAN HISTORY 1–2 (1959).

63 Edwin L. Godkin, *The Rights of the Citizen*, SCRIBNER'S MAG., July 1890, at 62.

64 Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970) ("We . . . categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another . . . . That we are often 'captives' outside the

day, the primary threat to individual privacy is the (mis)use of technology that permits private businesses and government agencies to have access to data about people's personal lives.

Over the last two decades, millions of Internet users have begun to surf the web and use commercial online services that cater to their needs for communication, information, and entertainment.[65] Internet users' personal information, especially consumer characteristics such as their earning level, address, and credit card use, is collected, processed and monetized without the individual's consent or even knowledge.[66] Many providers of online services record users' search history, browsing habits, shopping preferences, geolocation data,[67] health and genetic profiles, and even information about their feelings.[68] Indeed, Google confirms this practice in its privacy policy: "We collect information to provide better services to all of our users—from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like."[69]

---

sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere . . . . The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain.").

65 In 2015 it was estimated that there were over 3 billion Internet users worldwide. *See Privacy Bridges*, *supra* note 22, at 10.

66 CEES J. HAMELINK, THE ETHICS OF CYBERSPACE 12 (2000) (arguing that "information itself becomes a commodity tradable on a global scale"). For an illustration, *see Internet Advertising Revenue Report*, IAB (Apr. 2016), www.iab.com/wp-content/uploads/2016/04/IAB_Internet_Advertising_Revenue_Report_FY_2015-final.pdf [https://perma.cc/28TH-TAYA].

67 Geolocation privacy has recently come into question in cases where "connected vehicles affect personal information privacy interests, primarily through misuse of personal data about individual people." *See* Dorothy Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1657–58 (2014) (highlighting that "a connected vehicle seems likely to be considered comparable to a cell phone").

68 Roberto Alberdeston, Erich Dondyk & Cliff C. Zou, *Click-Tracking Blocker: Privacy Preservation by Disabling Search Engines' Click-Tracking*, U. CENT. FLA. 2 (2014), www.cs.ucf.edu/~czou/research/clickTrackBlocker-globecom14.pdf [https://perma.cc/336H-6ZGT].

69 *See Privacy Policy*, GOOGLE, www.google.com/policies/privacy [https://perma.cc/QL46-FZEB].

On the other hand, the validity of the consents obtained by multi-page end-user license agreements is questionable. It is hardly conceivable that silence, pre-ticked boxes, or inactivity could constitute valid consent.[70] On January 21, 2019, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), France's data watchdog, imposed a record €50 million fine (approximately $55 million) on Google for having failed to implement adequate measures to meet the requirements of the GDPR.[71] The Commission ruled that Google did not provide enough information to users about its data consent policies and did not give them enough control over the way their information is used.[72]

According to surveys, people who experience such threats to their privacy develop a higher awareness of the value of their personal information.[73] Privacy matters to society at large because it contributes to the "building and maintaining of relationships and the support of a more just, democratic, and tolerant society."[74] According to an interdisciplinary study, privacy includes protection from the overreach of social interaction; affirmation of self-ownership,

---

[70] GDPR, *supra* note 17, recital 32 ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her . . . . Silence, pre-ticked boxes or inactivity should not therefore constitute consent."). In this vein, see also the recent decision handed down by the ECJ on October 1, 2019 in Case C-673/17, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände—Verbraucherzentrale Bundesverband e.V. 2019 E.C.R. 801, ¶¶ 49, 65 (Oct. 1, 2019) (holding that the consent which a website user must give to the storage of and access to cookies on his or her equipment is not validly constituted by way of a pre-checked checkbox. Thus, the user must actively submit her or his approval for cookie storage).

[71] *See* Deliberation of the Restricted Committee SAN–2019–001 of 21 January 2019 Pronouncing a Financial Sanction Against Google LLC, CNIL 3 (2019), https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf [https://perma.cc/7USD-DVTS].

[72] *Id*. at 15–24.

[73] A recent survey indicates that eight out of ten Americans have concerns about the privacy of their financial and personal records. *See Nearly Half of Americans Say ID Theft Likely to Cause Them Financial Loss in the Next Year: AICPA Survey*, ASS'N INT'L CERTIFIED PUB. ACCT. (Apr. 3, 2018), www.aicpa.org/press/pressreleases/2018/nearly-half-of-americans-say-id-theft-likely-to-cause-them-finan.html [https://perma.cc/JPE8-YTRP].

[74] Trina J. Magi, *Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature*, 81 LIBR. Q. 187, 206 (2011).

moral agency, and freedom of choice; prevention against the victimization of people through categorization and being misjudged out of context; and the possibility for an individual to make a fresh start.[75]

A "fresh start" is nevertheless getting more and more difficult. Through data matching, data mining, and de-anonymization, technology leads to the creation of potentially massive "digital dossiers." The problem is that most people lack the legal tools allowing them to monitor and protect their personal information, or to cost-effectively redress the privacy breaches when they occur.[76] The usual minor efforts people make to defend their privacy online are often unsuccessful or rather effortlessly by-passed.[77] Given these developments, fairness seems more clearly than ever to dictate against placing the burden of privacy protection solely on the data subject.

In April 2015, a 31-year-old woman from Naples, Italy used WhatsApp to send a series of sex videos to five people, including her boyfriend.[78] In these videos she can be seen, in a drunken state, performing sex acts with various unidentified men. The videos were soon shared and uploaded onto several adult websites. However, this woman was subjected to more than voyeurism. She unwillingly became a notorious figure as her picture appeared on t-shirts, as websites parodied her, and as she was called shameful names. She decided to put up a fight. After unsuccessfully struggling for months to have the videos removed from the Internet, she went to court, arguing that the videos had been uploaded onto public websites without her consent.[79] By that time, she was no longer able to live a

---

[75] *Id*.

[76] Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1100 (1999) (highlighting that "these may be the worst of times for privacy, in that there appears to be so little of it. Yet these may also be the best of times, because the collective sense that privacy is being lost appears to be generating a cultural backlash").

[77] J.J. Sylvia IV, *Little Brother: How Big Data Necessitates an Ethical Shift from Privacy to Power*, *in* CONTROVERSIES IN DIGITAL ETHICS 13, 26 (Amber Davisson & Paul Booth eds., 2016) (pointing out that "big data-driven decision-making is able to sway easily the population at large without their having realized it"); Roger Clarke, *Internet Privacy Concerns Confirm the Case for Intervention*, 42 COMM. ACM 60 (1999).

[78] James Reynolds, *Italy's Tiziana: Tragedy of a Woman Destroyed by Viral Sex Videos,* BBC (Feb. 13, 2017), https://www.bbc.com/news/world-europe-38848528 [https://perma.cc/FJ5Y-8QYL].

[79] *Id.*; *see also* Tribunal of Naples (Nord), November 3, 2016, in Diritto dell'Informazione

normal life. On September 7, 2016, a Neapolitan court ordered the sex videos to be removed from various websites and search engines.[80] However, the court also ordered her to pay €20,000 ($22,700) in legal costs, which was all too much for her, especially as she had only a modest income.[81] Here are the words of her mother who, on September 13, 2016, had gone to work at the local town hall while her daughter stayed home: "My sister-in-law called me, and in a calm voice told me to come home; when I got here I saw the police, the ambulance, and I quickly understood. My sister-in-law tried to pick her up and save her. My neighbors didn't allow me to get out of my car. I almost fainted. They didn't want to let me into this house. I wasn't even able to see her for a last time. The day she died, my life ended."[82]

This happened in Europe, but such tragic events where the ongoing public availability of accurate information about an identifiable person leads to significant injustice without sufficient countervailing public benefits are happening everywhere, and often at mass level, with increasing regularity. The 2014 hacking of the online accounts of several celebrities, including Oscar winner Jennifer Lawrence, leading to the posting of their nude photographs online, is one of the numerous examples that happened in the United States.[83]

Although those are not without criticisms or reservations,[84] many methods have been used in the United States to remedy

---

e dell'Informatica 243 (2017) (commented by Matteo Montanari).

80 Reynolds, *supra* note 78. Before the final decision, the court ordered the websites to remove the videos on September 7, 2016. *Id.*

81 *Id*.

82 For more information on this case, see UMBERTO AMBROSOLI & MASSIMO SIDERI, DIRITTO ALL'OBLIO, DOVERE DELLA MEMORIA 1 (2017).

83 Ellie Davis, *Jennifer Lawrence on Dealing with Her Nude Photo Leak*, VOGUE (Nov. 21, 2017), www.vogue.co.uk/article/jennifer-lawrence-apple-hack-nude-images [https://perma.cc/2JBH-3NX9].

84 For criticisms or reservations see, e.g., William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 400–01 (1960) (arguing that "the privacy cases do go considerably beyond the narrow limits of defamation, and no doubt have succeeded in affording a needed remedy in a good many instances not covered by the other tort." He concludes that "it is here, however, that one disposed to alarm might express the greatest concern over where privacy may be going").

privacy breaches or data misuse[85] since Warren and Brandeis drew attention in 1890 to the necessity to set up protection against invasion of privacy. They argued that "inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[86]

Today, individual privacy is governed by constitutional provisions, federal and state statutes, regulations, and voluntary industry guidelines of practice that apply to the public and private sectors in different ways.[87] Plaintiffs seeking to vindicate privacy rights through litigation can select their causes of action from a range of tort claims.[88] Defamation creates a cause of action to protect one's reputation from false claims.[89] Intrusion upon seclusion creates a cause of action to protect one from the intentional invasion into a person's solitude or private area through, for instance, "eavesdropping, peeping through windows or surreptitiously opening another's mail."[90] Public disclosure of private facts is a cause of action against one that disseminates generally unknown private information, even if it is true.[91] A plaintiff may sue for misappropriation, which is using another's name, likeness, or other personal attributes without permission for exploitative purposes.[92] In some states, a plaintiff can bring a claim for false light if a defendant publishes information that places the subject in a highly offensive light.[93] As Professor Schwartz noted, "in a defamation action, the plaintiff complains that

---

85 Solove, *supra* note 60, at 77; Ieuan Jolly, *Data Protection in the United States: Overview*, PRAC. L., http://us.practicallaw.com/6-5020467 [https://perma.cc/3NLZ-UPV7].

86 Warren & Brandeis, *supra* note 50, at 195.

87 Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661, 668 (1999).

88 Joseph A. Page, *American Tort Law and the Right to Privacy*, *in* PERSONALITY RIGHTS IN EUROPEAN TORT LAW 38 (Gert Brüggemeier, Aurelia Colombi Ciacchi & Patrick O'Callaghan eds., 2010).

89 3 RODNEY A. SMOLLA, SMOLLA AND NIMMER ON FREEDOM OF SPEECH § 23:6 (2019).

90 *Id.* § 24:6.

91 *Id*. § 24:5.

92 *Id*. § 24:4.

93 *Id*. § 24:3.

the defendant's statement has diminished his reputation; the statement's falsity comes in by showing that this diminution is not justified. In a false light action, the defendant's falsehood brings about a mismatch or conflict between the plaintiff's actual identity and his identity in the minds of others, a conflict that itself can be offensive or disorienting."[94]

Intellectual property laws provide another mechanism to regulate information flows, and to mediate, problematize, or resolve tensions that may arise between freedom of speech and privacy. To take the fight against revenge porn in the United States as an example, copyright law can favor either the perpetrator or the victim, depending on the facts.[95] Copyright law compounds the violation of the victim's privacy if the perpetrator has photographed or filmed the images and therefore owns the right to distribute and reproduce them.[96] On the other hand, copyright law equips the victim with a powerful tool to fight back against the perpetrator if, as is often the case, the victim was the one who recorded the images and thus owns the distribution and reproduction rights.[97]

In the EU, too, there are several ways to resolve the inherent conflict between copyright and freedom of expression.[98] The ECJ has recently been questioned by the German Supreme Court as to whether, in the absence of an applicable copyright exception, fundamental rights like freedom of expression and freedom of information should permit the disclosure or unauthorized use of military reports that have been distributed to selected members of the Parliament as "classified documents."[99] In its decision handed down on

---

94 Gary T. Schwartz, *Explaining and Justifying a Limited Tort of False Light Invasion of Privacy*, 41 CASE WESTERN RES. L. REV. 885, 898 (1991).

95 17 U.S.C. § 201 (2012).

96 *See* Danielle Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 360 (2014).

97 Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422, 439 (2014).

98 *See* Jonathan Griffiths*, European Union Copyright Law and the Charter of Fundamental Rights—Advocate General Szpunar's Opinions in (C-469/17)* Funke Medien*, (C-476/17)* Pelham GmbH *and (C-516/17)* Spiegel Online, 20 ERA F. 35, 38 (2019).

99 Case C-469/17, Funke Medien NRW GmbH v. Bundesrepublik Deutschland, 2018 E.C.R. 870, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=207024&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1948409 [https://perma.cc/K4E4-UVVA]. On the facts and the opinion of Advocate

July 29, 2019, the ECJ ruled that "freedom of information and freedom of the press, enshrined in Article 11 of the [EU] Charter, are not capable of justifying, beyond the exceptions or limitations provided for in [the European Copyright Directive], a derogation from the author's exclusive rights of reproduction and of communication to the public."[100] Thus, just as in the United States, neither freedom of expression nor freedom of the press constitutes an autonomous ground to override the exclusive rights of a copyright holder, unless an exception or a limitation listed in the Copyright Directive is applicable.[101]

On the other hand, reflecting the high value placed on freedom of speech in American and European cultures, courts in both jurisdictions have restricted privacy torts in order to protect that freedom.[102] Thus, even though privacy torts can be invoked to deal with the publication of false or unknown information, they do not offer an adequate mechanism to protect true personal information from unwanted dissemination.[103] Furthermore, while copyright protects content created by the subject, it does not include non-creative uses of the work.[104]

None of the torts or protective mechanisms discussed above address in a coherent way the issue of the unconsented publication of true personal information. There are three main reasons for this. First, most privacy violation cases are based solely on hypothetical future harm and, in the absence of sufficient evidence proving direct

---

General see Stijn van Deursen & Thom Snijders, *The Court of Justice at the Crossroads: Clarifying the Role for Fundamental Rights in the EU Copyright Framework*, 49 INT'L REV. INTELL. PROP. & COMP. L. 1080 (2018) (highlighting the differences between the approaches taken by the ECJ and the ECtHR on that matter).

100 *See* Case C-469/17, at ¶ 64.

101 Council Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, 2019 O.J. (L 130).

102 Quin Landon, *The First Amendment and Speech-Based Torts: Recalibrating the Balance*, 66 U. MIAMI L. REV. 157, 165 (2011).

103 Paul A. Freund, *Privacy: One Concept or Many*, *in* PRIVACY & PERSONALITY 188, 188 (Ronald Pennock & John W. Chapman eds., 1971).

104 For more information and the recent developments, see R. Anthony Reese, *Copyrightable Subject Matter in the "Next Great Copyright Act*, 29 BERKELEY TECH. L.J. 1489 (2015).

or actual harm, courts tend to dismiss data breach claims.[105] Second, the disclosure or use of information on the Internet is often covered by the website's terms of use. Even though those are seldom read and even less often understood, Section 230 of the Communications Decency Act immunizes websites for the content published on their sites: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[106] Third, privacy breaches do not end with the intrusion. Often subsequent republication on the Internet by third parties causes more harm than the original breach.[107] Nevertheless, since in most instances the First Amendment protects the right to discuss and report on matters of public interest, the latter protects most republishers.[108]

Needless to say, the Constitutional Convention could not have foreseen the evolution in communication technology when it ratified the First Amendment in 1791.[109] However, as Justice Sotomayor has highlighted, "[T]he premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[110] The U.S. Supreme Court Justice's concern became more pronounced with the growing use of social media tools, live-streaming video, and direct messaging.

---

105 Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 534 (D. Md. 2016).

106 47 U.S.C. § 230 (2018).

107 Mills and Harclerode illustrate the impact of republication with a stunning example: "In 2016, a group of Russian hackers used a spear phishing attack to breach the email account of John Podesta, the chairman of Hillary Clinton's 2016 presidential campaign. This initial intrusion, the original publication of the emails on Wikileaks, and the subsequent republication of the emails on almost every news site imaginable played a substantial—but largely immeasurable—role in Donald Trump's defeat of Hillary Clinton in November 2016." Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion and the Modern Data Breach*, 69 FLA. L. REV. 771, 776–77 (2018).

108 *But see* The Bankruptcy Code, 11 U.S.C. § 700 (protecting a person who has filed for bankruptcy by prohibiting public and private actors to hurt that person's future as a result of the divulgation of the information); The Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (protecting individuals from the willful and/or negligent inclusion of inaccurate information in their credit report and to prevent unwarranted invasion of privacy).

109 On the evolution of First Amendment doctrine, see Thomas W. Joo, *The Worst Test of Truth: The "Marketplace of Ideas" as Faulty Metaphor*, 89 TULANE L. REV. 383 (2014).

110 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Social media serves, at first sight, similar functions of informing and entertaining as traditional media.[111] Indeed, just having access to a computer makes it possible to record and publish images, experiences, ideas, and emotions, and reach millions of people at the same speed as television, although not always with the depth of a newspaper or magazine.[112] In the legal context, the creation of such a "sociological archive" raises difficult normative problems regarding the interpretation of matters of public concern and the limits of self-determination. Can the loss of self-determination itself be deemed sufficient evidence of the harm suffered by the plaintiff in a breach of privacy case? To what extent does the First Amendment apply to social media content or Internet search engines?[113] Can a right to know be sustained as a matter of constitutional principle?[114] Can all active Internet users and social media enthusiasts be considered as their own "press" in terms of the First Amendment? If the question is answered in the negative, what kind of content deserves the application of the special press privileges? If the question is answered in the affirmative, does the protection offered by the First Amendment not swallow the right to privacy?

---

[111] An author defines social media as "the many relatively inexpensive and widely accessible electronic tools that enable anyone to publish and access information, collaborate on a common effort, or build relationships." DHIRAJ MURTHY, TWITTER: SOCIAL COMMUNICATION IN THE TWITTER AGE 7 (2013).

[112] A leading trust study has revealed that search engines and social media platforms play a key role in explaining why the media is the least trusted institution. *2018 Edelman Trust Barometer Reveals Record-Breaking Drop in Trust*, EDELMAN (Jan. 22, 2018), www.edelman.com/news-awards/2018-edelman-trust-barometer-reveals-record-breaking-drop-trust-in-the-us [https://perma.cc/3MQ7-4VS4]. *See also* Craig Silverman, *Lies*, *Damn Lies, and Viral Content*, TOW CTR. DIGITAL JOURNALISM 146 (Sept. 5, 2017), https://academiccommons.columbia.edu/doi/10.7916/D8Q81RHH [https://perma.cc/MG83-TU6A].

[113] Oren Bracha notes that "the claim that First Amendment protection extends to ranking of search results may appear well founded, at least as a matter of positive law." Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629, 1685 (2014). However, according to the author, "on closer examination, this certainty disappears, [since] the First Amendment has a vital role to play in limiting governmental power." *Id*. at 1632.

[114] See Lillian R. BeVier, *An Informed Public, an Informing Press: The Search for a Constitutional Principle*, 68 CAL. L. REV. 517 (1980) (concluding that "the first amendment does not in principle guarantee that a well-informed citizenry with the press as its constitutionally appointed information gathering agent are values of affirmative, independent constitutional significance").

In an evolving technological landscape, new ways of legal thinking are needed in order to respond properly to these pressing questions. In another common law jurisdiction, Justice Mann of the High Court of England and Wales issued an unusual and inspiring decision in the recent Mirror News Paper phone hacking case, *Gulati*.[115] This decision defines loss as the diminution of the plaintiff's right to privacy itself and thus considerably broadens the scope of privacy tort:

> Those values (or interests) [i.e., the protection of the individual's informational autonomy] are not confined to protection from distress, and it is not in my view apparent why distress (or some similar emotion), which would admittedly be a likely consequence of an invasion of privacy, should be the only touchstone for damages. While the law is used to awarding damages for injured feelings, there is no reason in principle, in my view, why it should not also make an award to reflect infringements of the right itself, if the situation warrants it. The fact that the loss is not scientifically calculable is no more a bar to recovering damages for 'loss of personal autonomy' or damage to standing than it is to damages for distress. If one has lost the right to control the dissemination of information about one's private life then I fail to see why that, of itself, should not attract a degree of compensation, in an appropriate case. A right has been infringed, and loss of a kind recognised by the court as wrongful has been caused. It would seem to me to be contrary to principle not to recognise that as a potential route to damages.[116]

While this decision does not solve all the normative problems when it comes to the limits of self-determination, it does show that a more liberal approach to privacy is possible. Whether American law or

---

[115] Gulati v. MGN Ltd. [2015] EWHC 1482 (Ch), ¶ 111, *available at* www.5rb.com/wp-content/uploads/2015/05/MGN-trial-jt-REDACTED.pdf [https://perma.cc/UK5N-HT8J].

[116] *Id*.

continental European law can provide the grounds upon which to base such an ingenious and original decision remains to be seen.

B. Gaps in Existing Data Protection Norms

The definitions of privacy and personal data, as well as the scope of their protections, have been subject to ongoing change as a result of rapid technological advances (e.g. genomic data) and globalization.[117] As exemplified by the recent complaint with the Federal Trade Commission ("FTC") alleging that Amazon's *Alexa* or similar devices violate the Children's Online Privacy Protection Act ("COPPA") because they collect and process personal data by recording kids' voice conversations,[118] these ongoing changes make it difficult to predict the outcome of the cases where data protection laws could apply. However, the evolution of the right to data protection has acquired distinctive and essentially stable characteristics that reliably distinguish it, to some extent, from the right to privacy. Data protection is about securing "personal data," rather than providing redress for "injury to [a] plaintiff's emotions and his [or her] mental suffering."[119] The Organization for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data defines personal data as "any information relating to an identified or identifiable individual (data subject)."[120]

In the EU, data protection is seen as a specific expression of the right to privacy,[121] and therefore specific rules set forth in the GDPR

---

[117] Magi, *supra* note 74, at 206 (concluding that "the term 'privacy' is difficult to define and perhaps best used as an umbrella term to describe a web of related concepts").

[118] *Request for Investigation of Amazon, Inc.'s Echo Dot Kids Edition for Violating the Children's Online Privacy Protection Act*, FTC (May 9, 2019), https://drive.google.com/file/d/1RptCGM-88t08xGj3CaxKMMbml7glT1EK/view [https://perma.cc/Q7AE-TEN2].

[119] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 958 (1989) (defining the purpose of privacy tort by referring to Froelich v. Adair, 516 P.2d 993, 997 (1973) and Hazlitt v. Fawcett Publications, Inc., 116 F. Supp. 538, 544 (D. Conn. 1953)).

[120] OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, art. 1(b) (2013), www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1 [https://perma.cc/MD9G-4N2C].

[121] Juliane Kokott & Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIVACY L.

regulate it.[122] In contrast, data privacy regulation in the United States is currently a kind of "hodgepodge,"[123] because it is not underpinned by a clear, unified right to privacy. Instead of a federal law regulating the way entities across all industries are allowed to collect and use consumer data, there is a horde of different laws applying to various issues and sectors of the economy. For example, COPPA regulates the protection of the privacy of children under the age of 13 in their interactions with online websites. Another example is the Gramm-Leach-Bliley Act ("GLBA"), which applies to financial institutions and establishes requirements designed to protect consumer data. Furthermore, the Health Insurance Portability and Accountability Act ("HIPAA") safeguards the privacy of individually identifiable health information.[124]

The Fair Credit Reporting Act ("FCRA")[125] was one of the first instances of data protection law passed in the digital age.[126] The FCRA has been amended several times since it was enacted in 1970. The 2013 amendment empowers consumers to dispute the completeness, accuracy, or fairness of information mentioned in a report and to request the correction or deletion of negative information found on a credit report if it is associated with the consumer's personal information.[127] Even if, at first sight, the scope of application of the

222, 222 (2013) (discussing "the relevant jurisprudence of Europe's two highest courts, the European Court of Human Rights in Strasbourg . . . and the CJEU, with regard to the differences between privacy and data protection").

122 Bart van der Sloot, *Legal Fundamentalism*: *Is Data Protection Really a Fundamental Right?*, *in* DATA PROTECTION AND PRIVACY: (IN)VISIBILITIES AND INFRASTRUCTURE 3 (Ronald Leenes et al. eds., 2017).

123 Glancy, *supra* note 22, at 359.

124 *See* United States v. Bormes, 568 U.S. 6 (2012); Nat'l Fed'n of Indep. Bus. V. Sebelius, 567 U.S. 519, 622 (2012); Watters v. Wachovia Bank, 550 U.S. 1 (2007).

125 15 U.S.C. § 1681 *et seq*. (2018).

126 On various occasions the U.S. Supreme Court has upheld and enforced this Act. *See Bormes*, 568 U.S. at 613; Sorrell v. IMS Health Inc., 564 U.S. 552 (2011); Safeco Ins. Co. of Am. V. Burr, 551 U.S. 47 (2007). Recent constitutional challenges to the FCRA have been rejected. *See* King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303 (E.D. Pa. 2012); *see also*, Memorandum of the United States of America in Support of the Constitutionality of § 1681c of the Fair Credit Reporting Act, King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303 (E.D. Pa. 2012) (No. 2:10-cv-06850-PBT), *available at* www.ftc.gov/sites/default/files/documents/amicus_briefs/shamara-t.king-v.general-information-services-inc./120508fcraking-gis.pdf [https://perma.cc/5NJW-XP5T].

127 15 U.S.C. § 1681(i)(a)(5)(A) (2012).

FCRA seems narrower than that of the GDPR, the protection it offers is actually very similar, as it grants American citizens a right similar to the right to erase conferred to EU citizens following *Google Spain*, provided that search engines can be classified as credit reporting agencies.[128]

Nevertheless, many types of data collection, such as databases used to target sales and marketing efforts and airline reservation data, fall outside the scope of these federal statutes.[129] In the United States, the FTC Act, which established the FTC and is the most wide-ranging federal data privacy regulation, partially fills the gap.[130] Indeed, the FTC is the primary regulatory body for data protection, even though it was not created for this specific purpose.[131] On the basis of Section 45 of the Act, the FTC regulates "[u]fair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[132] Within this framework, a misleading representation, practice, or omission will

---

[128] And they might well be, since, besides collecting information a user actively gives when typing a search query, search engines also gather information through the use of cookies or similar technologies. *See generally* Mark T. Andrus, *Constitutional Issues in Granting Americans a "Right to Dispute" Personal Information with Search Engines Akin to the Existing Remedy Afforded to Europeans Via Europe's Right to Be Forgotten*, BUS. L. TODAY (Sept. 19, 2018), www.americanbar.org/groups/business_law/publications/blt/2016/11/07_andrus [https://perma.cc/BWB7-SZ6F].

[129] Stephen Cobb, *Data Privacy and Data Protection: U.S. Law and Legislation*, ESET 6 (2016), https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf [https://perma.cc/DT9Q-TD75].

[130] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2233 (2015).

[131] Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 814 (2011).

[132] 15 U.S.C. § 45(a)(1) (2006). *See generally* Federal Trade Commission Act of 1914, Pub. L. No. 63-203, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41–58 (2006)) (FTC's primary goal was to "prevent persons, partnerships, or Corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."). *See generally* Clayton Antitrust Act of 1914, Pub. L. No. 63-212, 38 Stat. 730 (codified as amended at 15 U.S.C. §§ 12–27 (2006) and 29 U.S.C. §§ 52–53 (2006)) (stating that one of the primary goals of the FTC was to prevent the acquisition of "the whole or any part of the assets of one or more persons engaged in commerce or in any activity affecting commerce," when the intention of the person seeking to acquire such assets was to lessen competition or to create a monopoly). *See* Serwin, *supra* note 131, at 814–15 ("FTC was originally created in 1914 in order to protect competition among businesses.").

be deemed "deceptive" and thus give rise to liability if it is "material," when viewed from the perspective of a reasonably acting consumer,[133] and a consumer acting in reasonable reliance on the material representation, practice, or omission would foreseeably suffer injury, loss, or harm in consequence of that reliance.[134] Thus, the FTC's authority to regulate consumer data protection in all industries not specifically targeted by federal law is based upon data subjects' deception.

Under Section 45, the FTC is able to sue companies that use deceptive practices. It can do so either on its own or upon referrals, from either EU data protection authorities or third-party private dispute resolution providers. Some critics argue that this system is slow and complicated and does not help consumers.[135] Moreover, although the FTC has obtained numerous settlements, including in some of the largest data breach lawsuits, the phrase "unfair or deceptive" clearly limits its authority. Federal courts have recently cast doubt on the FTC's right to deal with personal data breaches. In *LabMD*, for instance, the Court of Appeals for the Eleventh Circuit ruled that "the [FTC's] complaint alleges no specific unfair acts or practices engaged in by LabMD."[136]

Examples of personal data breaches are multiple, but the recent cases of *Equifax*, *Facebook*, and *Ashley Madison* are the most striking ones in the United States. Equifax, one of the nation's largest credit reporting companies, has recently revealed a massive data breach that affected more than 148 million Americans.[137] In its statements made in 2017 and 2018, the company reported that the names and dates of birth of approximately 146.6 million people

---

133 *See* Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Congressman John D. Dingell, Chairman, House Comm. on Energy Commerce 1 (Oct. 14, 1983), www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [https://perma.cc/SR2L-PCHF].

134 *See id.*

135 *See* Serwin, *supra* note 131, at 816.

136 LabMD*,* Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1230 (11th Cir. 2018). *See also* Fed. Trade Comm'n v. AT&T Mobility LLC, 883 F.3d 848 (9th Cir. 2018).

137 *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-559, REPORT TO CONGRESSIONAL REQUESTERS: DATA PROTECTION ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH (2018), https://www.gao.gov/assets/700/694158.pdf [https://perma.cc/5HPA-8R2J].

were exposed, as well as 145.5 million Social Security numbers, the address information for 99 million people, the gender data for 27.3 million people, 20.3 million consumers' phone numbers, 17.6 million driver's license numbers, 1.8 million email addresses, 209,000 credit card numbers and expiration dates, and 97,500 tax ID numbers.[138]

In another data privacy scandal in March 2018, Facebook declared that the personal data of 87 million users worldwide had been collected through an app from November 2013 to May 2015 and transferred to Cambridge Analytica, a political consulting firm.[139] Millions of users' data was accessed and exploited, without the data subjects' consent, to create politically useful profiling and micro-target citizens, giving campaign groups the ability to connect with individual voters.[140]

Another example is the *Ashley Madison* data breach.[141] In July 2015, an anonymous hacker group calling itself the Impact Team hacked into Ashley Madison, an online cheating website and threatened to publish the stolen information unless Ashley Madison was permanently shut down.[142] The parent company, Avid Life Media, refused and, as a result, the hackers uploaded about thirty gigabytes of stolen data on the dark web. This data included the personal information of the site's users—data the website had promised not to keep—as well as information about the company, such as financial data, and employee salary information. The users whose data was published have faced several problems during the litigation

---

138 *See* Equifax Inc., Equifax's Statement for the Record Regarding the Extent of the Cybersecurity Incident Announced on September 7, 2017, https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm [https://perma.cc/BUM9-X8XW].

139 Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/F8SJ-AF5T].

140 *Id*.

141 *See* Zetter, *supra* note 14; Krebs, *supra* note 14; Baraniuk, *supra* note 14.

142 *Id*.

process, including an order issued by the federal district judge appointed to lead the multidistrict litigation to publicly disclose the class representatives' names.[143]

The number of persons affected by the cases mentioned above and the procedural difficulties they encountered in remedying the damage caused by the alleged data breaches can serve as an illustration of the burdens that the current legal system imposes on an individual seeking to redress the misuse of personal information in a timely and satisfactory manner.[144] On the one hand, as Chief Justice John Roberts pointed out in *Riley*, "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[145] On the other hand, both the hacked businesses and the individual victims are under the impression that the judicial system should be adaptable to technological developments.[146] As hackers are most often located outside the country's jurisdiction, identifying who is liable is a difficult task.[147] The victims' frustration rises even further due to their inability to prevent bloggers, the media and others from copying, republishing, or commenting on the stolen data. This is, so to speak, part of most hackers' plans: republication of the data after the hack to harm their

---

143 Order Granting Final Approval of Settlement, Cy Pres Distribution, and Award of Attorney's Fees and Service Awards to the Class Representative, *In re* Ashley Madison Customer Data Sec. Breach*,* Litig.*,* No. 4:15-md-02669 (E.D. Mo. Nov. 20, 2017), *available at* https://www.moed.uscourts.gov/sites/moed/files/documents/415md2669-0383.pdf [https://perma.cc/5RQ9-ML9L].

144 Thomas Nagel, *The Shredding of Public Privacy*, *in* CONCEALMENT AND EXPOSURE 27 (2002) (discussing "the culmination of a disastrous erosion of the precious but fragile conventions of personal privacy in the United States over the past ten or twenty years").

145 Riley v. California, 573 U.S. 373, 403 (2014).

146 *See, e.g.*, Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/N7D3-FJST] ("We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy.").

147 Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), www.scientificamerican.com/article/tracking-cyber-hackers/?redirect=1 [https://perma.cc/62FN-X46N] (noting that "an attack may appear to come from a particular server or computer, but this does not mean the attack originated at that device").

target. Freedom of expression and freedom of the press protect the republication of hacked data, leaving a data subject very little opportunity to seek relief once the media have gotten a hold of stolen data.[148] However, the fact that technology now allows data to be dispersed across many operational systems and disseminated over wide geographical distances should not make data any less worthy of the protection.[149] Indeed, as many as 88% of Americans would support the adoption of the so-called "right to erasure of personal data."[150]

II. LEGISLATIVE EFFORTS TO ADDRESS THE CHALLENGES TO DATA PRIVACY

Recent legislative efforts at the state and federal levels in the United States indicate that Americans are as concerned about data privacy as are Europeans, even though the latter have implemented more laws on that subject.[151]

A. Recent Developments Following the CCPA

The tendency to reinforce data privacy protection on the basis of new rules instead of relying on the existing ones have become more noticeable in the EU than in the United States, particularly with the adoption of the GDPR.[152] However, privacy protection and data security, which include the right to erase, are not only on the EU agenda. It seems that the developments in data privacy protection in the EU have been used to ratchet up standards in the United States.

In May 2014, reporting serious concerns about the privacy implications of "people search" services that permit access to large

---

148 Mills & Harclerode, *supra* note 107, at 784.

149 Former Supreme Court Chief Justice John Roberts similarly highlighted that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection." *See Riley*, 573 U.S. at 403.

150 Rebecca Heilweil, *How Close Is An American Right-To-Be-Forgotten?*, FORBES (Mar. 4, 2018), www.forbes.com/sites/rebeccaheilweil1/2018/03/04/how-close-is-an-american-right-to-be-forgotten/#37851d33626e [https://perma.cc/FWY9-JT68].

151 *See "Take Back Your Data" Campaign*, ACLU, https://www.aclu.org/other/take-back-your-dataprivacy-rights-pocket-card [https://perma.cc/6RL5-UWB7].

152 W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAWYER 221 (2017).

amounts of an individual's personal information based solely on a search of that individual's name, the FTC recommended to the Congress a broader privacy protection.[153] The FTC advocated for legislation that would require data brokers to[154]:

> (1) allow consumers to access their own information;
> (2) allow consumers to opt out of the use of the information;
> (3) clearly disclose to consumers the data brokers' sources of information, so that, if possible, the consumer can correct his or her information at the source; and
> (4) clearly disclose any limitations of the opt out, such as the fact that close matches of an individual's name may continue to appear in search results.[155]

The FTC's recommendation highlights the fact that current American privacy law does not efficiently address the issue of data protection. The general public shares this point of view. A 2017 Harris poll of more than one thousand Americans found that eight in ten adults are concerned about the ability of businesses to safeguard their financial and personal information.[156] The 2017 Norton Cyber Security Insights Report revealed the cost of data security failures in financial terms: cybercrime cost American consumers

---

[153] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 54 (2014), www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/CYT4-8ZER].

[154] According to the OECD, "data brokers are firms that gather and merge aggregated information on individuals that is then sold for various uses such as employment background checks, the issuing of credit and for law enforcement purposes." *See Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en [https://perma.cc/56BB-F8Y7].

[155] FED. TRADE COMM'N, supra note 153, at ix.

[156] AICPA, *supra* note 73. This survey was conducted by The Harris Poll by telephone within the United States between October 12 and 15, 2017, among 1,006 adults. Figures for age, sex, race/ethnicity, education, region and household income were weighted (using data from the Current Population Survey) where necessary to bring them into line with their actual proportions in the population.

$19.4 billion of their own money in 2017.[157] This high cost importantly shows that American businesses taken as a whole have failed to implement the principles known collectively as "Privacy by Design."[158] These principles reflect the idea that privacy measures and privacy enhancing technologies should be embedded directly into the design of information technologies and systems, providing a proactive rather than a reactive approach.[159]

In order to respond to this concern, some state lawmakers in the United States enacted several measures taking European data protection concept as a model. That is why, before turning to the recent developments in the United States, it is necessary to mention briefly the process of the adoption of the GDPR, which makes Privacy by Design a mandatory provision for businesses.[160] The effort to enact a new data protection law in the EU goes back to November 2010 when, after years of reflection, consultation, and debates, the Vice-President of the European Commission and EU Justice Commissioner, Viviane Reding, announced a reform designed to make Europe the standard setter for modern data protection rules in the

---

[157] *2017 Norton Cyber Security Insights Report*, SYMANTEC (2018), www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-united-states-en.pdf [https://perma.cc/5AFZ-B8QZ].

[158] For other reasons companies increasingly felt unwilling to follow self-regulatory privacy standards, see Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 362–64 (2015).

[159] For more information on Privacy-by-Design, see Ann Cavoukian & Jeff Jonas, *Privacy by Design in the Age of Big Data*, PRIVACY BY DESIGN (June 8, 2012), https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf [https://perma.cc/E9AW-VM6C]; JEROEN VAN REST ET AL., DESIGNING PRIVACY-BY-DESIGN, ANNUAL PRIVACY FORUM 2012: PRIVACY TECHNOLOGIES AND POLICY 55 (2012).

[160] *See* GDPR, *supra* note 17, art. 25 ("Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing . . . , the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures . . . to protect the rights of data subjects. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.").

digital age.[161] In January 2012, the European Commission revealed its proposal to adopt more concrete remedies, as well as its proposal to create a far-reaching new privacy right—the "right to erase."[162] If certain conditions regarding the data are met,[163] a data subject may exercise the right to erase and thereby place an obligation on the data controller to check the conditions for erasure of the specified personal data "without undue delay."[164] In 2014, the ECJ held for the first time that EU citizens have a right to erase.[165] Over the last few years, Reding's speech and this decision constraining Google's public disclosure of private facts have widely been debated.[166] The right to erase was then codified in Article 17(2) of the GDPR, which creates a stronger and more cohesive data protection law than the 1995 Data Protection Directive.[167] The GDPR entered into force on

---

[161] Viviane Reding, Vice-President of the European Comm'n, Privacy Matters—Why The EU Needs New Personal Data Protection Rules, Speech at the European Data Protection and Privacy Conference (Nov. 20, 2010), europa.eu/rapid/press-release_SPEECH-10-700_en.pdf [https://perma.cc/SXW4-AEMS]. It is worth noting that at that time, several European countries developed laws protecting privacy rights and implemented the concept of a right to be forgotten into their national privacy policy. *See, e.g.*, BVerfGE 65, 1 BvR 209/83, Dec. 15, 1983, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html [https://perma.cc/5CQT-N9YC] (judgment of the German Constitutional Court ruling that individuals are entitled to determine which information about themselves is known to others). For more information on this topic, see Gloria González Fuster, *The Surfacing of National Norms on Data Processing in Europe*, 74 Cambridge L.J. 245–47 (2014).

[162] *Commission Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012).

[163] GDPR, *supra* note 17, art. 17.1.

[164] *Id*. The timescale of appropriate delay is "about a month." *See Everything You Need to Know About the "Right to Be Forgotten,"* GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ [https://perma.cc/LSF5-WNAN].

[165] Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 717.

[166] For comments on Reding's speech, see ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 4, 232 (2015); Alexandra Rengel, PRIVACY IN THE 21ST CENTURY 146 (2013); Rosen, *supra* note 36. On *Google Spain*, see generally Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017 (2016); Post, *supra* note 35; Julia Powles, *The Case That Won't Be Forgotten*, 47 LOY. U. CHI. L.J. 583 (2015).

[167] *See generally* Francoise Gilbert, *The Right to Erasure or Right to Be Forgotten: What the Recent Law, Cases, and Guidelines Mean for Global Companies*, 18 J. INTERNET L. 13 (2015).

May 25, 2018 and replaced the Directive,[168] which had not fully harmonized national privacy laws within Europe.[169]

The legislative efforts in the EU are not limited to the adoption of the GDPR. To replace the 2002 e-Privacy Directive, on January 10, 2017, the European Commission issued a proposal for a Regulation on Privacy and Electronic Communications designed to update current rules to reflect technological developments, and to adapt the rules to fit within the GDPR's regulatory framework.[170] This proposal aims at strengthening the rules on the protection of electronic communications data, for example by requiring that browser settings should disable cookies by default.[171] Such a configuration would allow Internet users to prevent other parties from

---

168 *See generally* GDPR, *supra* note 17.

169 Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 71 (2019).

170 *Commission Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 final (Jan. 10, 2017).

171 *See id*. recital 24 ("For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others [sic], require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed."). In this vein see also *id.* art. 10 ("Information and Options for Privacy Settings to Be Provided: 1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. 2. Upon installation, the software shall inform the end-user about

storing or processing their information without consent. This browser default setting would harmonize well with the Privacy by Design approach implemented in the GDPR, which makes preservation of privacy a central part of the architecture of Internet products and services. Moreover, the Amendments also extend from six months to twelve months the periodic intervals at which users are given the opportunity to withdraw or confirm their consent regarding the use of their information. Finally, both the European Parliament and the Council agreed on the necessity to implement by default "Do-Not-Track" mechanisms in browser settings. Such mechanisms enable users to signal content providers their preference towards behavioral advertising.[172] In line with the GDPR, the Proposal expressly stated that a valid "opt-in" consent must be obtained from the user in order to send unsolicited electronic communications such as e-mails, push notifications, or SMS.[173]

These recent developments in data privacy outside American borders have already influenced, to some extent, the data protection policies of online companies such as eBay or Amazon, social media platforms like Twitter, and search engines such as Google.[174] The

---

the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.").

[172] Martin Degeling et al., *We Value Your Privacy . . . Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, NETWORK & DISTRIBUTED SYSTEMS SECURITY (NDSS) SYMP. 2019 1, 3 (2019), https://arxiv.org/pdf/1808.05096.pdf [https://perma.cc/3ALY-YKSY].

[173] As mentioned on the official website of the EU, in case of electronic marketing to existing customers regarding the company's own similar products or services, such a consent is not required, on condition that, for each marketing communication, customers have the opportunity to withdraw their consent. This withdrawal right must be available free of charge. *See generally Data Protection and Online Privacy*, YOUR EUROPE: EUROPEAN UNION (June 14, 2019), https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm [https://perma.cc/452L-QJP7].

[174] *See Ebay's Commitment to GDPR*, EBAY, https://www.ebayinc.com/company/privacy-center/gdpr/ [https://perma.cc/6P4X-PAAK]; *General Data Protection Regulation (GDPR)*, AMAZON WEB SERVICES, https://aws.amazon.com/compliance/gdpr-center/ [https://perma.cc/Y6UM-87Y7]; *What is Twitter's Approach to the GDPR?*, TWITTER, https://gdpr.twitter.com/en/faq.html [https://perma.cc/EF7Y-T3PN]; *Our Commitment to GDPR*, GOOGLE, https://privacy.google.com/businesses/compliance/#!?modal_active=none [https://perma.cc/EP2S-T2S3]. *See also* Ashley Stenning, *Gone but Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impacts of Data Breaches*,

changes in data protection policies have also had a significant impact on other business areas in the United States, as well as in many other countries. EU law has indeed become a *de facto* standard for American technology companies in respect of data flows into the United States.[175] For example, cloud-based-services offered by American providers to individuals in the EU have been modified to be in line with GDPR privacy policy requirements.[176] The evolution of data protection in Europe has also influenced the path of American public policy. Nevertheless, consequent changes would not be a mere reaction to an apparent economic threat from the old continent, but rather the result of a number of converging technological, social, and legal changes in the field of privacy and data protection in the United States.[177] The alarmist consequences about the loss of privacy reported by the new Harris poll mentioned above illustrate this phenomenon.[178]

As a response to these consequences, and considering the GDPR as a model, on June 28, 2018, the state of California adopted the CCPA, which goes into effect on January 1, 2020. In addition to the CCPA, the Privacy Rights for California Minors in the Digital World Act, effective as of January 1, 2015, prohibits the collection of personal data of minors that would be shared with third parties for the purpose of advertising or marketing.[179] The most significant feature of the California legislation is the provision granting to minors a right to be forgotten.[180] A California resident who is under 18 years of age is allowed to request the permanent deletion of any online content that is collected and stored about them by an online service company.[181]

---

18 SAN DIEGO INT'L L.J. 129, 157 (2016) (confirming that "American-based websites are already conforming their policies and actions to the privacy laws of the EU").

175 Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Rights to Data Protection*, 23 MAASTRICHT J. EUR. & COMP. L. 815, 841 (2016).

176 *See* W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. L. 221, 223 (2017).

177 *See* Priscilla M. Regan, *The Globalization of Privacy: Implications of Recent Changes in Europe*, 52 AM. J. ECON. & SOC. 257, 270 (1993).

178 *See* AICPA, *supra* note 73.

179 CAL. BUS. & PROF. CODE § 22580–22582 (West 2015).

180 *Id*. § 22581(a)(1).

181 *Id*.

The CCPA is the most rigorous general privacy and data security law in the United States. Even if, at first sight, the fact that this California law applies only to consumers makes the CCPA's scope of application appear narrower than the GDPR's scope,[182] the effective territorial reach of the CCPA will not be limited to California. Since the headquarters of hundreds of high technology companies are in the region commonly known as "Silicon Valley," the CCPA will reach their operations in most, if not all, of the states.[183]

The CCPA incorporates in California law a large number of personal data rights found in the GDPR. It gives Californian consumers an effective means of control over their personal information. The CCPA defines "personal information" as any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[184] According to the Act, particularly (1) common identifiers that, when used, may allow the identification of the individual to whom the information in question may

---

[182] *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1978.140(g). A resident is defined as "every individual who is in the State for other than a temporary or transitory purpose, and every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose." CAL. REV. & TAX. CODE § 17014 (West 2019). Any "business" gathering the "personal information" of a consumer as defined above should comply with the CCPA. CAL. CIV. CODE § 1978.140. The definitions of "business" and "personal information" require explanation as well. The term of "business" is described fairly broadly, and it applies to any industry, whatever the method used to collect data, which is not the case at the federal level. CAL. CIV. CODE § 1978.140(c). To be more exact, the CCPA applies to any company that collects the personal information of Californians, is for profit, does business in California, and exceeds $25 million in gross revenue; handles the personal information of 50,000 or more consumers, devices or households; or derive more than 50% of their annual revenue from selling consumers personal information. CAL. CIV. CODE §§ 1798.140(c)(1)(A)-(C). Hence, even though it will only be a state law, its broad jurisdictional reach means that it will actually apply to companies throughout the United States and around the world.

[183] Fortune 1000 cited, particularly, Adobe Systems, Advanced Micro Devices (AMD), Agilent Technologies, Alphabet Inc. (formerly Google Inc.), Apple Inc., Applied Materials, Cisco Systems, eBay, Electronic Arts, Facebook, Hewlett Packard Enterprise, HP Inc., Intel, Intuit, Juniper Networks, KLA Tencor, Lam Research, LSI Logic, Maxim Integrated Products, NetApp, Netflix, Nvidia, Oracle Corporation, Salesforce.com, Sanmina-SCI, Symantec, Tesla, Inc., Visa Inc., Western Digital Corporation, Xilinx. *Fortune 1000 (2019)*, SOMEKA, https://www.someka.net/excel-template/fortune-1000-excel-list/ [https://perma.cc/77RC-27DW].

[184] CAL. CIV. CODE § 1798.140(o)(1).

relate;[185] (2) electronic network activity information, including, browser histories, search history, and any information regarding a consumer's interaction with a Web site, application or advertisement;[186] (3) audio, electronic, visual, thermal, and olfactory information;[187] and (4) geolocation data are considered personal information.[188] Moreover, the CCPA provides that any "inferences" drawn from various data elements of personal information "to create a profile about a consumer reflecting the consumer's preference, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes" constitutes personal information.[189]

The adoption of the CCPA constitutes a non-negligible shift in the nation's data privacy regime. First, the Act entitles consumers to know the categories and specific pieces of personal information that a business has collected within the past year, sold to a third party, or disclosed to another person for a business process.[190] Second, the CCPA requires companies to provide consumers choice to opt out of the sale of their personal information, and companies are not allowed to discriminate, with respect to prices or services, against consumers who opt out.[191] The personal information of individuals under sixteen years cannot be sold, unless the latter exercise their "right to opt in"—i.e. they allow such sharing.[192] Third, the Act states that businesses have to be open about their privacy policies, disclosing for example a list of the types of personal information gathered, sold, or disclosed to third parties over the last twelve months.[193] Fourth, the Act provides a private right of action seeking damages or relief for consumers whose personal data "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain

---

185 *Id.* § (1)(A).
186 *Id.* § (1)(F).
187 *Id.* § (1)(H).
188 *Id.* § (1)(G).
189 *See id.* § (1)(K).
190 *Id.* § 1798.100(a).
191 *Id.* § 120(a).
192 *See id.* § 120(d).
193 *See id.* § 130(a)(5)(C)(i).

reasonable security procedures and practices appropriate to the nature of the information."[194] The statute also provides that violations can result in Attorney General investigation and enforcement under the Business and Professions Code if, after a thirty-day period, the business has not managed to cure the alleged violation.[195] Fifth, the Act entitles consumers to a "right to delete," allowing them to request that a business delete any information collected about the consumer.[196] A business that receives such a request must delete the information gathered and direct any "service providers" to do the same.[197] The CCPA nevertheless provides that the "right to delete" cannot be exercised in a small number of circumstances, such as when the information is needed to complete a particular transaction for the consumer, to detect security incidents, or to ensure the right of another consumer to exercise his or her free speech.[198]

A similar balance between diverse interests can be found in the GDPR as well. Recital 65 of the GDPR details the circumstances in which an organization's right to process someone's data might override an individual's right to erase. An asserted interest in processing data takes priority over the right of erasure if the data:

> 1) is used to exercise the right of freedom of expression;
> 2) is used to comply with a legal ruling or obligation;
> 3) is used to perform a task carried out in the public interest or when exercising an organization's official authority;
> 4) is necessary for public health purposes and its divulgation serves the public interest;
> 5) is necessary to perform preventative or occupational medicine (provided the data is processed by a health professional who is subject to a legal obligation of professional secrecy);
> 6) represents important information that serves the public interest, scientific research, historical

---

194 *See id.* § 150(b)(1).
195 *See id.* § 155(a).
196 *See id.* § 105(a).
197 *See id.* § 1798.105(c).
198 *See id.* § 1798.105(d).

> research, or statistical purposes and where erasure of the data would be likely to hinder the achievement that was the goal of the processing; and
> 7) is used to establish of a legal defense or other legal claims.[199]

This comparison of the CCPA and the GDPR reveals that, even if the rules aimed at protecting personal data are relatively recent, the legislative and regulatory developments in the United States and the EU point toward a harmonization process of data protection standards through the propagation of data protection laws and their substantive convergence. In this sense, rules on both sides of the Atlantic have been mutually shaping each other. The efforts in the United States at the state level to bring about a comprehensive data protection reform in conformity with the GDPR recognizes the GDPR's potential to be a legislative guide for a greater globalization.[200]

Since the start of 2019, the "California Effect," whereby legislatures take the CCPA as a model for their own data protection and privacy bills, has been felt in many states, including Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, New York, Washington, and North Dakota.[201] Hence, at least at the state level, several American lawmakers set a new balance on the basis of the GDPR enabling diverse interests to coexist in an environment that fosters public awareness of—and respect for—privacy/data protection. The new laws set forth expansive catch-all rules and standards that provide general data security guidelines to address previously neglected regulatory areas or issues.[202] That is why, for the time being, it seems that there is no "race to the bottom" in global standards. Far from seeking to lower data protection requirements, state legislatures are consolidating the effective alignment of standards with the GDPR. That is not the end of the problems, but it is the beginning of solutions.

---

199 *See* GDPR, *supra* note 17, recital 65.

200 For a similar view, see generally Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP. L. & SEC. REP. 508 (2008).

201 *See generally* Marmor et al., *supra* note 42.

202 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 848–49 (5th ed. 2014).

B. Need for Large-Scale Projects

Although state-level laws and regulations in the United States, such as the newly adopted CCPA, have benefits, they also give rise to significant challenges. Even if most state unfair or deceptive acts and practices statutes empower state Attorneys General to issue rules and regulations interpreting the law and establishing prohibited conduct,[203] effective enforcement of the new rules at the state level does demand more cooperation and coordination between the FTC and state Attorneys General.

State laws will likely remain ineffective for two reasons.[204] The first reason behind the inefficiency of state-level regulations is that they are subject to federal law preemption.[205] Indeed, constitutional challenges can—and do—occasionally invalidate state privacy laws.[206] The second fact explaining the ineffectiveness of state-level regulations is that they often conflict with one another. Even if states have started to apply data protection rights as a component of the right to self-determination in general and of consumer law in particular, this process is too erratic to establish a national regime in line with rising international standards.[207] Differences in state laws are likely affect consumers negatively, because the same type of information might well be protected in one state while remaining unprotected in another.[208] Some states set higher data protection standards than others, and discrepancies also exist between state and federal levels, with the result that businesses can face considerable

---

[203] Cary Silverman & Jonathan L. Wilson, *State Attorney General Enforcement of Unfair or Deceptive Acts and Practices Laws: Emerging Concerns and Solutions*, 65 KAN. L. Rev. 209, 212 (2016).

[204] Jolly, *supra* note 85, at 2.

[205] Schwartz, *supra* note 34, at 1976–77.

[206] *Id.* at 1977 ("It struck down a Vermont law that prohibited the sale, disclosure, and use of pharmacy records by 'detailers,' who used the information to help target doctors for the sale of prescription pharmaceuticals.") (referencing Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2659–60 (2011)).

[207] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/3ZQZ-RTGA].

[208] *See* Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law,* TEACH PRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ [https://perma.cc/MQ2K-2W78].

difficulty in determining the correct standard of compliance.[209] Moreover, the choice of protecting privacy at the state level is not the best solution for businesses, because of the enormous transaction costs involved in complying with different sets of rules across several jurisdictions, especially when each has its own unique matrix of privacy protections.[210] Presently, cost-benefit analysis might lead American businesses to restrict their commercial activities to their local areas.[211]

These issues, which are critical to consumers and businesses alike, make the adoption of a comprehensive federal privacy legislation not only more desirable, but also more realistic in the context of the twenty-first century's data protection challenges. If the federal government were to enact a data protection law along the lines of the EU's regime, companies could accomplish international transfers and rapidly expand into international markets.[212]

While various members of Congress have proposed bills to create a federal data privacy statute or data protection board,[213] nothing has passed through both the Senate and the House.[214] On February 26, 2019, the Consumer Protection and Commerce Subcommittee of the House Energy and Commerce Committee held a hearing titled "Protecting Consumer Privacy in the Era of Big Data." Subcommittee chair Jan Schakowsky (D-IL) referred to the inefficacy of the system in her opening statement: "Reports of the abuse of personal information undoubtedly give Americans the creeps. . . . Without a comprehensive federal privacy law, the burden has fallen completely on consumers to protect themselves. This

---

209 Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111, 1118, 1123 (2017).

210 Cobb*, supra* note 129, at 3, 5.

211 *Id*. at 8.

212 Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 837, 842–44 (1960) (arguing that, without transaction costs, commercial actors will always favor the course of action most effective in allocating wealth).

213 Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?*, 27 CATH. U. J.L. & TECH. 77, 99 (2018).

214 Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2d Sess. 2014); Data Security Act of 2014, S. 1927, 113th Cong. (2d Sess. 2014); Data Security Act of 2015, S. 961, 114th Cong. (1st Sess. 2015). *See also* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 367–68 (2015).

must end."[215] One day later, the Senate Committee on Commerce, Science, and Transportation held a hearing on "Policy Principles for a Federal Data Privacy Framework in the United States." During his opening address, Senator Roger Wicker (R-MS) said the following: "It is clear to me that we need a strong, national privacy law that provides baseline data protections, applies equally to business entities—both online and offline—and is enforced by the nation's top privacy enforcement authority, the Federal Trade Commission."[216]

The FTC already works to protect privacy and improve data security in the online market,[217] particularly when it comes to behavioral advertising. For example, the FTC has issued the following guidance:

> The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.[218]

However, the compliance with its recommended standards, particularly with those aiming at regulating behavioral advertising through

---

[215] *Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection and Commerce*, 116th Cong. (2019) (statement of Jan Schakowsky, Chair, S. Comm. on Consumer Protection and Commerce) https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/0226%20JS%20Opening%20Statement%20CPC%20Data%20Hearing.pdf [http://perma.cc/C3XU-55A4].

[216] Tom Ramstack, *US Senate Seeks Federal Data Regulation That Could Preempt Colorado Law*, COLO. POL. (Feb. 28, 2019), www.coloradopolitics.com/news/us-senate-seeks-federal-data-regulation-that-could-preempt-colorado/article_3ca59efa-3b59-11e9-afee-4b5826c3cbe4.html [https://perma.cc/N7V3-NNT4].

[217] *See, e.g.*, FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2018, www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/835Q-BNXZ].

[218] FED. TRADE COMM'N, A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, vii (2010), www.ftc.gov/os/2010/12/101201privacyreport.pdf [https://perma.cc/J8RR-3LQT].

a "Do Not Track Mechanism,"[219] is voluntary.[220] This is the reason why the FTC's requirements fall far short of creating a compelling incentive for online companies to honor a consumer's Do Not Track request. In order to remedy this issue, on May 21, 2019, Senator Hawley introduced the Do Not Track Act, which aims to give consumers the power to block online companies from collecting any data beyond what is necessary for the companies' online services.[221]

The FTC's authority and investigative tools would become more effective if political opinion coalesced into a nascent consensus that consumers must be given more control over the collection and use of their information, and if that consensus actually led to the passage of a federal data privacy act. According to Hyman and Kovacic, "Congress would eliminate the FTC's jurisdictional limitations and give it the authority to enforce privacy across the board—including against not-for-profit institutions."[222] Humerick argues that "[E]ven if Congress does not ease the burden, the FTC must promulgate a rule that establishes a standard for general data protection and requires industry agencies to monitor data protection compliance throughout the States."[223] If the political will does develop to invigorate the FTC's role in data protection, further study into whether

---

[219] *See* Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 283 (2012) (defining "tracking" as an "activity [which] involves a third party, largely unfamiliar to the user, collecting and processing information about her based on her browsing activity on various unrelated websites in order to compile an individual profile, which will be used to facilitate the targeting of ads") (citing *What Does "Do Not Track" Mean?*, CTR. DEMOCRACY & TECH. 3, 5 (2011), http://www.cdt.org/files/pdfs/CDT-DNT-Report.pdf [https://perma.cc/Y6GU-4AKZ]).

[220] Alexander Nill & Robert J. Aalbert, *Legal and Ethical Challenges of Online Behavioral Targeting in Advertising*, 35 J. CURRENT ISSUES & RES. ADVERT. 126, 137 (2014).

[221] *Senator Hawley to Introduce Legislation to Give the American People a "Do Not Track" Option*, JOSH HAWLEY (May 20, 2019), www.hawley.senate.gov/senator-hawley-introduce-legislation-give-american-people-do-not-track-option [https://perma.cc/VH4W-E6GV].

[222] David Hyman & William E. Kovacic, *Implementing Privacy Policy: Who Should Do What?*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 1117, 1142 (2019).

[223] *See* Humerick, *supra* note 213, at 82 (citing Alex Y. Seita, *Globalization and the Convergence of Values*, 30 CORNELL INT'L L.J. 429, 472–76 (1997) (discussing how the increasing globalization of trade and the importance of data collection serve as impetuses for the United States to adopt federal privacy standards to ease international data transfer relations)); Amanda C. Border, *Untangling the Web: An Argument for Comprehensive*

the FTC could use antitrust law as an appropriate tool to encourage businesses to offer better privacy protections would become particularly valuable.[224] The potential importance of antitrust action in this area arises from the non-rivalrous nature of data:

> [D]ata is 'non rivalrous' in the sense that access to data by an operator does not, in and of itself, preclude access by other operators. Multi-homing by customers as well as the diversification of services offered by a single firm provides opportunities for the concurrent collection of user-specific data. However, accessing this data in the first place may be conditioned on the capacity for the firm to build a sufficiently large customer base, which in turn depends on the extent to which network and experience effects as well as scale economies act as [a potential] barrier to entry[, or] an element of such barrier and thus as a factor which limits competition.[225]

This point of view is shared by numerous American lawyers, too.[226] A former Commissioner at the FTC, for instance, highlighted the fact that the entrenched sector-specific businesses' "data-driven"

Data Privacy Legislation in the United States, 35 SUFFOLK TRANSNAT'L L. REV. 363, 384 (proposing that "the United States should shift away from its "piecemeal approach" to data privacy").

224 *See generally* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 2–3 (2016); D. Daniel Sokol & Roisin E. Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129 (2016); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121 (2015).

225 *Competition Law and Data,* AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT 28, 53 (May 10, 2016), www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=1EC8E78261D1A13AC50E59F111CCCDB0.2_cid371?__blob=publicationFile&v=2 [https://perma.cc/J387-MZCX].

226 *See, e.g.*, Daniel Castro & Michael Steinberg, *Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help,* CTR. FOR DATA INNOVATION 17 (2017), www2.datainnovation.org/2017-open-apis.pdf [https://perma.cc/6YZR-R2V9] (arguing it would be more appropriate to focus on "the entrenched sector-specific businesses that can use their exclusive access to key industry data to restrict competition in their industry" than "on large tech companies, such as Facebook or Google") (citing Joe Kennedy, *"The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown,"* INFO. TECH. & INNOVATION FOUND. (2017), http://www2.itif.org/2017-data-competition.pdf [https://perma.cc/CC6C-SNS5].

conducts may operate as a barrier to entry, and as such justify enforcement actions.[227]

In the United States, most experts and academics too support the idea of an explicit individual right to regulate consumer data privacy.[228] In addition, a bipartisan agreement appears to have developed concerning the need to fill the gap in data protection at federal level. The Former First Chief Privacy Officer for the U.S. Department of Homeland Security, Nuala O'Connor, has offered this explanation of the need to codify a federal law:

> Most Western countries have already adopted comprehensive legal protections for personal data, but the United States—home to some of the most advanced, and largest, technology and data companies in the world—continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data. U.S. citizens and companies suffer from this uneven approach—citizens because their data is not adequately protected, and companies because they are saddled with contradictory and sometimes competing requirements.[229]

There is nevertheless no general consensus as to what specifically the solution would be.[230] The devil will be in the details. If Congress actually decides to pursue legislative action, it will have

---

[227] Terrell McSweeny & Brian O'Dea, *Data, Innovation, and Potential Competition in Digital Markets—Looking Beyond Short-Term Price Effects in Merger Analysis*, CPI ANTITRUST CHRON. 2 (Feb. 2018), www.competitionpolicyinternational.com/wp-content/uploads/2018/02/CPI-McSweeny-ODea.pdf [https://perma.cc/GPW9-N443].

[228] *See, e.g.*, Jugpreet Mann, *Small Steps for Congress, Huge Steps for Online Privacy*, 37 HASTINGS COMM. & ENT. L.J. 365, 388 (2015); Alex Y. Seita, *Globalization and the Convergence of Values*, 30 CORNELL INT'L L.J. 429, 472–76 (1997).

[229] O'Connor, *supra* note 207.

[230] *See* Stephen P. Mulligan, Chris D. Linebaugh & Wilson C. Freeman, *Congressional Research Service Report: Data Protection Law: An Overview,* CONG. RES. SERV. 1, 3 (Mar. 25, 2019), https://fas.org/sgp/crs/misc/R45631.pdf [perma.cc/AXL6-MTJK] ("[C]oncerns that existing federal laws are inadequate ha[ve] led many stakeholders to argue that the federal government should assume a larger role in data protection policy. However, at present, there is no consensus as to what, if any, role the federal government should play, and any legislative efforts at data protection are likely to implicate unique legal concerns such as preemption, standing, and First Amendment rights, among other issues.") (citations omitted).

to deal with serious issues, such as: What protection for what categories of data? For what data uses will customer have opt-out rights? What about opt-in rights? Should there be a private right of action? Despite all these uncertainties, the adoption of a federal privacy law creating a nationwide standard clearly would not only bring the European and American systems closer to each other, at least at the systematic level, but would also increase convergence between different regulatory systems within the United States.

Two main reasons lie behind the desire in the United States to craft a unified law that would broaden the scope of data protection.[231] Firstly, the current rules governing privacy—both at federal and state level in several states—do not offer protection sufficient to the task of responding effectively to concerns associated with today's and tomorrow's data breaches, and do not meet the expectations of consumers that are insufficiently informed of how their data is used.[232] Secondly, even though some courts create new exceptions to existing rules or broaden the existing exceptions, the case law is still far from settled regarding how to remedy the data protection shortfall, and does not provide a satisfactory level of legal certainty.[233] The climate of legal uncertainty caused by varying national approaches contributes to increasing the costs of legal services on which businesses rely in order to comply with different rules.[234] As

---

[231] *Id*. at 54–61.

[232] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 1, 17–19 (2019), www.gao.gov/assets/700/696437.pdf [https://perma.cc/9SX7-PLC9] (citing public opinion surveys about public concerns over the protection of consumer data); *see also* Mary Madden, *Public Perception of Privacy and Security in the Post-Snowden Era,* PEW RES. CTR. (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ [http://perma.cc/M79V-W349] (highlighting that 64% of Americans think that the government should get more involved in regulating advertisers' privacy practices).

[233] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) ("The concept of harm stemming from a data breach has confounded the lower courts. There has been no consistent or coherent judicial approach to data-breach harms.").

[234] *Small Businesses Data Regulation and Responsibility*, CONNECTED COMMERCE COUNCIL 39 (2019), https://connectedcouncil.org/wp-content/uploads/2019/04/Small-Businesses-Data-Regulation-and-Responsibility.pdf [https://perma.cc/JRN2-HLFX] (citing that "state laws would vary too much to make it financially possible for small companies to adhere to").

a recent survey shows, the modernization of existing national legislation would provide legal certainty not only for consumers but also, and particularly, for business.[235]

Legal scholars and policy analysts have already raised ideas, made proposals, and described implementation scenarios in respect of future data protection law at the national level.[236] Although many think that an EU-style law would not be compatible with the culture and structure of American law,[237] conformity with the fundamental principles and rights of the GDPR would eliminate, to some extent, barriers to the transfer of personal information from one continent to another, as well as barriers to the operation of the global economic system.[238] Indeed, data's free-flowing nature requires an all-embracing legislation.[239] However, this view does not imply that the role of national courts in developing a case-by-case test to deal with privacy and data protection claims should be disregarded. Legislative frameworks set standards which leave room for courts to decide under what circumstances a data breach occurs.

III. COURTS' EFFORTS TO DEVELOP AN EFFECTIVE AND BALANCED PROTECTION

In addition to the intention on both sides of the Atlantic to adopt a more liberal approach to data privacy by way of legislative reform, the court decision in the United States and the EU have emphasized to protect private information as an aspect of the principle of self-determination. The tests applied by the ECJ to public disclosure of

---

235 *Id.* at 40.

236 *See, e.g.*, Kerry, *supra* note 22.

237 Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment*, 61 B.C. L. Rev. (forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441502 [https://perma.cc/J97G-99S2].

238 According to a study, cultural differences are mediated by regulations. *See* Steve Bellman, Eric Johnson, Stephen Kobrin & Gerald Lohse, *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 30 INFO. SOC'Y 1, 7 (2004).

239 *See* Cory Bennett, *Lawmakers See Momentum for Data Breach Legislation*, HILL (Jan. 27, 2015, 12:34 PM), http://thehill.com/policy/cybersecurity/230867-data-breach-bill-is-achievable-goal [https://perma.cc/56WZ-63WU]; *see also* ROLF H. WEBER & DOMINIC N. STAIGER, TRANSATLANTIC DATA PROTECTION IN PRACTICE 134 (2017) (pointing out that "in addition to the industry protection, legal minimum standards should be set on a[n] international level in order to ensure that basic measures and protection are implemented").

private facts are not significantly different than those applied by American courts. On the contrary, the case analysis shows that their practical concerns and approaches are rather similar.

A. Practical Concerns and Approaches in the EU: Beyond Google Spain

My study of EU law leads to two main findings. First, the ECJ's approach is based on a case-by-case examination of different fundamental rights and other interests. Second, this approach permits the right to privacy to coexist with the right to access information and with freedom of expression, as evidenced by a statistical inference based on data derived directly from Google.

1. Case-by-Case Appraisal

One might wonder whether the parallel I have drawn between the American and European legislative efforts to establish new standards regarding the scope of the right to privacy and data security[240] is supported by court-made law developed in the long-standing struggle to find a fair solution to various data protection issues. I will demonstrate that, although the ECJ has broadened the scope of data protection in the EU, it did not ultimately lead to an imbalance that would unduly favor data protection over other rights. To get a full picture of the application of data protection law in the EU, *Google Spain*[241] should be read in tandem with the recent *Manni* decision.[242] Comparing this study with the case law established by American courts would illuminate the similarities and differences of both approaches. I will first sketch briefly *Google Spain*, which held that EU law gives persons a right to erase personal information from the Internet.[243] I will then study *Manni*, where the ECJ highlighted

---

240 *See supra* Part III.

241 Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317.

242 Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

243 *Google Spain* has been the object of several studies in the United States and Europe. The comments cover a wide range of opinions. Whereas some call the decision "clinically insane" others argue that the decision "indicates a renewed and vehement commitment to

that the right to erase established in *Google Spain* is not unconditional and needs to be balanced against conflicting interests. The contrast between these two decisions gives a full picture of the Court's implementation of the balancing test and reveals the conditions in which the right to erase is to be exercised.

The *Google Spain* case started with a Spanish citizen, Mario Costeja González, filing a complaint with the Spanish Data Protection Agency against a local newspaper, *La Vanguardia*, and Google Spain.[244] In 1998, the newspaper had published announcements about real estate auctions held to secure repayment of Mr. González's social security debts.[245] The newspaper's auction notices had also been made available on the web.[246] In November 2009, Mr. González asked the local newspaper to delete the pages or alter them so that his personal data would no longer be displayed.[247] Over ten years after their publication, Mr. González argued that these pages were no longer necessary because "the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant."[248] He also contacted Google Spain, asking for the links to the articles in question to be removed so that his personal data no longer appeared in Google Search results.[249] Google Spain forwarded the request to Google Inc. Subsequently, Mr. González sought the help of the Spanish Data Protection Agency. The latter rejected his claims against the newspaper,[250] but upheld those against Google Spain and Google Inc.[251]

---

the protection of privacy . . . ." *See* Interview with David Hoffman, Director of Security Policy and Global Privacy Officer, Intel, STEPTOE CYBERBLOG (Sept. 3, 2014), www.steptoe.com/images/content/5/9/v1/5905/SteptoeCyberlawPodcast-032.mp3 https://perma.cc/Q3WN-CEZQ; Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos*, 14 HUM. RTS. L. REV. 761, 776 (2014).

244 Case C-131/12, Google Spain SL, at ¶ 14.

245 *Id*.

246 *Id*.

247 *Id*. at ¶ 15.

248 *Id.*

249 *Id.*

250 *Id.* at ¶ 16.

251 *Id.* at ¶ 17.

Google Spain and Google Inc. separately appealed to Spain's high court.[252] Google Inc. argued that the company was not within the scope of the EU Directive 95/46/EC.[253] Google Spain argued that it was not responsible for the algorithm of the search engine, since, according to the Company, its activity is limited to providing support to Google Inc.'s advertising activity, which is separate from its search engine service.[254] Google Spain and Google Inc. both argued that there was no processing of personal data within the search function; that even were there processing, neither Google Inc. nor Google Spain could be regarded as a data controller; and that in any event, the data subject did not have the right to erasure of lawfully published material.[255] Google Inc., in turn, referred to the ECJ, among others, the preliminary question as to whether an individual has the right to request that their personal data be removed from search results.[256] The ECJ ruled that the European citizens are entitled to request that search engines that collect personal data for profit, such as Google, should remove links to private information (e.g. a person's full name) when asked, as long as the information is no longer relevant.[257] Based upon this decision, Google Inc. created a form that enables European citizens to request to have outdated and irrelevant search results on European domains removed.[258] The Court did not define exactly what is newsworthy in terms of time, but it seems that a ten-year time period—from 1998 to 2009—is enough for lay persons' social security debts to become irrelevant for public interest.[259] In the United States, the FCRA requires, in a

---

252 *Id.* at ¶ 18.

253 *Id*. at ¶ 22.

254 *Id*. at ¶ 51.

255 *Id.* at ¶ 22.

256 *Id.* at ¶ 20.

257 *Id.* at ¶ 62.

258 *See* Christopher Kuner, *Google Spain in the EU and International Context*, 22 MAASTRICHT J. EUR. & COMP. L. 158, 159–64 (2015) (discussing the jurisdictional implications of the decision).

259 Case C-131/12, Google Spain SL, at ¶ 98. The ECJ ruled that "having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list." The 16-year period mentioned by the ECJ covers a period of time from the claim to the decision. *Id.*

similar way, credit agencies to remove most *negative credit information* after seven years and bankruptcies after seven to ten years, depending on the kind of bankruptcy.[260]

In *Google Spain*, the ECJ did not require the publisher (*La Vanguardia*) to remove the content that the plaintiff had sought to have deleted.[261] The right to erase personal information does not alter the content on the web, but merely the online search results.[262] In his opinion, the Advocate General confirmed that "the Directive does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests."[263] The resource thus does not disappear; it remains active and can be further circulated, although it becomes less accessible.[264] In fact, when read in tandem with the recent Google decision handed down by the ECJ in September 2019,[265] the ruling basically applies to search engines within the borders of the EU the current rights to rectification, erasure, blocking, and objection which already existed in the previous Data Protection Directive 95/46/EC.[266] It is not necessary to find that links are prejudicial to the data subject.[267] The Court decided that the fundamental right to privacy should be considered more important than the economic interest of a commercial

---

260 15 U.S.C. § 1681c(a)(2) (2018).

261 Case C-131/12, Google Spain SL, at ¶¶ 16, 98.

262 Melanie Dulong de Rosnay & Andres Guadamuz, *Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving*, 6 RESET SOCIAL SCI. RES. INTERNET ¶ 3 (2016).

263 Case C-131/12, Google Spain SL, at ¶ 108.

264 Samuel W. Royston, *The Right to Be Forgotten: Comparing U.S. and European Approaches*, 48 ST. MARY'S L.J. 253, 273–74 (2016) (arguing that "de-linking is not censorship because the data is deleted from the search engine but not from the entire Internet[, which] is tantamount to allowing a book to remain on library shelves but redacting all of the pages").

265 Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), 2019 E.C.R. 772, ¶ 73.

266 Melanie Dulong de Rosnay & Andres Guadamuz, *supra* note 262, at ¶ 26.

267 Case C-131/12, Google Spain SL, at ¶ 99 ("[I]t should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject.").

intermediary, provided the data subject is not seen as a public person or a person who assumes a role in public life.[268]

In the EU, the essence of commercial activity is that the offering of goods and/or services "must be capable of being carried on, at least in principle, with a view to profit."[269] Neither the legal status of the entity engaged in the activity nor the way in which it is financed affects the law's recognition of the commercial nature of the activity.[270] Moreover, in principle, no commerce occurs when the state carries performs activities that the market could not provide.[271] The question as to whether the entity organization or group which disseminates information to the public carries out a commercial activity seems to have played a central role in the field of data protection law. That data protection law developed via this route becomes apparent when *Google Spain* is read in tandem with *Manni*. Although both deal with the right to erase, the economic activities of Google differentiate this case from *Manni*, where a government agency disclosed official information about a registered business.[272]

Even though the American scholarly community has not given close consideration to *Manni*, understanding this case is essential to forming a complete picture of the right to erase in the EU.[273] In 2007, Salvatore Manni, the sole director of a building company that was building a tourist complex in Italy, brought an action before the Italian Court of Lecce against the Lecce Chamber of Commerce.[274]

---

[268] *Id*. ("However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.").

[269] *See* Joint Cases C-180/98 and 184/98, Pavlov v. Stichting Pensioenfonds Medische Specialisten, Opinion of Advocate-General Jacobs ¶ 107, 2000 E.C.R. I-6451.

[270] Case C-118/85, Comm'n v. Italy, 1986 E.C.R. 413, http://curia.europa.eu/juris/celex.jsf?celex=61985CC0118&lang1=en&type=TXT&ancre= [https://perma.cc/G5C9-WXYQ]; Case C-35/96, Comm'n v. Italy, 1998 E.C.R. I-3851.

[271] *Report on Competition in Professional Services*, at ¶ 67(1), (COM) (2004) 83 final (Sept. 2, 2004).

[272] Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, ¶ 24, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

[273] *Id.* at ¶ 26.

[274] *Id.* at ¶ 24.

He argued that the properties built in that complex were not selling because the company register specified that Mr. Manni had been the sole director and liquidator of another building company that went bankrupt in 1992 and was wound up in 2005.[275] Mr. Manni also alleged that, although he asked for his personal data to be removed from the company register, the Chamber of Commerce had not complied.[276] He therefore petitioned the Court for an order requiring the Chamber to erase, anonymize, or block the information connecting him to the bankrupt company.[277] He also sought compensation for the damage he suffered as a result of the injury to his reputation.[278]

The Court of Lecce agreed with Mr. Manni's argument that naming the sole director of the insolvent company which had been liquidated over ten years ago was neither necessary nor useful.[279] Accordingly, the Court ordered the Chamber of Commerce to anonymize—but not remove—the data about the Applicant's involvement with the no-longer existing company.[280] The Court stated that the company register could not permanently maintain the connection between a natural person and an insolvent company "after an appropriate period" following the liquidation, even if Italian law does not specify a maximum term for the retention of data published in the company register.[281] According to the Court, there is no particular public interest in the disclosure of such an outdated information.[282] Finally, the Court ordered the Chamber to pay compensation for the harm done to the Applicant's reputation, in recognition of the fact that the latter had successfully demonstrated that several potential buyers had brought an end to their negotiations as a result of their discovery of the information regarding the Applicant's involvement in the bankrupt company.[283]

In 2012, the Chamber of Commerce appealed this decision directly to the Italian Supreme Court—the appeal concerned the

---

275 *Id.*
276 *Id.* at ¶ 25.
277 *Id.* at ¶ 26.
278 *Id.*
279 *Id.* at ¶ 27.
280 *Id.*
281 *Id.* at ¶ 28.
282 *Id.*
283 *Id.* at ¶ 27.

interpretation of the right to erase and its limits.[284] *Manni* raised the issue of how a person's right to erase should be balanced against the prevailing public interest in disclosing data concerning business organizations.[285] According to the Supreme Court, public registers, such as the company register, promote the creation of sound commercial and social relations through providing a reliable record of information essential to defining the legal status of commercial entities and to ensuring the legal validity of their dealings.[286] Nevertheless, the Supreme Court recognized the importance of the right to erase, as it had been acknowledged by the ECJ in *Google Spain*, as an important method of protecting personal identity.[287] Faced with this dilemma, the Italian Supreme Court referred preliminary questions to the ECJ.

In its preliminary decision, the ECJ held that the Applicant's right to erase could not supersede the right of the public to be informed.[288] Furthermore, the ECJ held that the disclosure of the Applicant's personal data kept in the company register by the Lecce Chamber of Commerce was lawful, because registering and disclosing this kind of official information protects third parties.[289] The ECJ reasoned that this interference with the Applicant's fundamental rights to a private life and the protection of personal data was not disproportionate, because company registers disclose only a limited amount of personal data, and because company executives are obligated to disclose their identity and function within a company, even one that stopped trading years ago.[290] The ECJ concluded that, in exceptional circumstances, when the data subject proves the existence of overriding and legitimate reasons to withhold disclosure, third parties might not be granted access to the data subject's personal information found in the company register.[291] However,

---

284 *Id.* at ¶ 29.
285 *Id.* at ¶¶ 43–44.
286 *Id.* at ¶ 43.
287 *Id.* at ¶ 37.
288 *Id.* at ¶ 63.
289 *Id.* at ¶¶ 49, 51, 60.
290 *Id.* at ¶ 60.
291 *Id.* at ¶ 64.

this exception was limited by the proviso that the company must have been dissolved for a sufficiently long period of time.[292]

As in *Google Spain*, the court did not specify when a period of time became "sufficiently long" following the embarrassing fact, in this case the dissolution of the Applicant's company. The ECJ held that, given the circumstances, it was not possible to identify an appropriate maximum retention period regarding personal data kept in publicly available registers.[293] Unlike U.S. law, EU law does not include any explicit regulation of personal data collected in public registers.[294] In the United States, the Federal Privacy Act establishes a Code of Fair Information Practice[295] that governs the collection, maintenance, use, and dissemination of personal identifiable information about individuals that is maintained in systems of records by federal agencies.[296] In the absence of a comparable privacy act at the EU level, the ECJ would have had to define the legitimate reasons for preventing the disclosure of information contained in the public record if it had ruled in favor of the Applicant. However, the ECJ did not address this issue, because it concluded that third parties had an overriding interest in having access to the public records regarding the Applicant's previous dealings and business history.[297]

---

[292] *Id.*

[293] *Id.* at ¶ 60.

[294] Even if there is no regulation at the EU level, member states have adopted fair information practices as law. *See, e.g.*, Directive 1995/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31–51 (EC).

[295] For the evolution of Fair Information Practices (FIPs), see generally ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY 1 (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [https://perma.cc/2B4C-D59P].

[296] 5 U.S.C. § 552a (2012); *see generally* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001).

[297] Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, ¶¶ 32, 50, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

In the EU, official public records of company details required by law are meant to show, at a glance, the whole history and management of a company as correctly and as objectively as possible.[298] Disclosing such records to the public, official registers are well positioned to play a neutral intermediary role in ensuring openness, transparency, and public availability of company data. This approach mirrors the one found in many states' public record acts[299] as well as in court opinions in the United States.[300]

The register is not the source of the information it provides and it has no control over the content of the information registered; its

---

[298] *See* Directive 2009/101, art. 2, of the European Parliament and of the Council of 16 September 2009 on Coordination Of Safeguards Which, For The Protection Of The Interests Of Members And Third Parties, Are Required By Member States Of Companies Within The Meaning Of The Second Paragraph Of Article 48 Of The Treaty, With A View To Making Such Safeguards Equivalent, 2009 O.J. (L 258/11) 11–19 (EC) [hereinafter Directive 2009/101] ("Member States shall take the measures required to ensure compulsory disclosure by companies as referred to in Article 1 of at least the following documents and particulars: (a) the instrument of constitution, and the statutes if they are contained in a separate instrument; (b) any amendments to the instruments mentioned in point (a), including any extension of the duration of the company; (c) after every amendment of the instrument of constitution or of the statutes, the complete text of the instrument or statutes as amended to date; (d) the appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law or as members of any such body: (i) are authorised to represent the company in dealings with third parties and in legal proceedings; it must be apparent from the disclosure whether the persons authorised to represent the company may do so alone or must act jointly; (ii) take part in the administration, supervision or control of the company; (e) at least once a year, the amount of the capital subscribed, where the instrument of constitution or the statutes mention an authorised capital, unless any increase in the capital subscribed necessitates an amendment of the statutes; (f) the accounting documents for each financial year which are required to be published . . . ; (h) the winding-up of the company; (i) any declaration of nullity of the company by the courts; (j) the appointment of liquidators, particulars concerning them, and their respective powers, unless such powers are expressly and exclusively derived from law or from the statutes of the company; (k) the termination of the liquidation and, in Member States where striking off the register entails legal consequences, the fact of any such striking off.").

[299] *See, e.g.*, CAL. GOV'T CODE § 6252(e) (2016) (defining the term "public records" broadly as "information relating to the conduct of the public's business [that is] prepared, owned, used, or retained by any state or local agency regardless of the physical form or characteristics").

[300] *See, e.g.*, Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 472–73 (1975) (allowing publication of rape victim's name already available in a criminal indictment).

only function is to enable third parties to ascertain information concerning the company in question.[301] That point distinguishes *Manni* from *Google Spain*. In fact, search engines do not have a passive attitude regarding information they make accessible.[302] Unlike public registers, search engines not only collect information from its source, but they also process the data.[303] On the basis of the algorithm they are using, search engines, as profit-making entities, refer only to certain web pages and data fields, and in a particular order when a specific term or name is entered.[304] In 2006, AOL imprudently released the search habits of 657,426 Internet users.[305] The records revealed the following:

> 90 percent of the total clicks went to sites on the first page of results;
> 74 percent of clicks went to the top five search results;
> the top result alone received 42 percent of all clicks.[306]

---

[301] Directive 2009/101, *supra* note 298, at recital 3.

[302] For an empirical approach, see Sounman Hong, *Does Google Distort Your 'Click'? Search Engines and the Emergence of Internet Monopolies* 22 (June 23, 2016), http://ssrn.com/abstract=2799664 [https://perma.cc/C497-Y4U6] ("[T]his study offered suggestive but compelling empirical evidence that search engines at least somewhat contribute to the emergence of Internet monopolies.").

[303] The ECJ defined in *Google Spain* the activity of a search engine as follows:

> [I]n exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves,' 'records,' and 'organizes' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results.

Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, 2014 E.C.R. 317, at ¶ 28.

[304] *See* Florent Thouvenin, Peter Hettich, Herbert Burkert & Urs Gasser, *Remembering and Forgetting in the Digital Age*, 38 L. GOV. & TECH. SERIES 59, 62 (2018).

[305] Following this incidence, AOL removed the search data from its site and apologized for its release. *See* Michael Barbaro & Tom Zeller Jr., *Web Searchers' Identities Traced on AOL*, N.Y. TIMES (Aug. 9, 2006), www.nytimes.com/2006/08/09/technology/08cnd-aol.html [https://perma.cc/8RJ4-WFW5].

[306] MATTHEW HINDMAN, THE MYTH OF DIGITAL DEMOCRACY 69 (2009).

These figures, confirmed by more recent studies,[307] show that search engine rankings affect the user's behavior. Higher ranked results tend to attract more attention and, therefore, have a higher chance of being accessed, whereas low ranked results may not be visited even if they are more relevant to the user's information need. This makes us understand why search engines, just like social media platforms, have a crucial role not only in forming attitudes on topics ranging from fingernail care trends to presidential elections, but also in influencing a person's perception of others and the judgments he or she formulates regarding them.[308]

Of course, this process of mutual influence alone cannot be held as evidence conclusive enough to apply the right to erasure. The ECJ pays close attention to the nature of the information in question, the public's interest in that information's disclosure, and the possible impact of such disclosure when determining whether or not the information in question may be made publicly available.[309] Here, too, it is possible to draw a parallel between the two sides of the Atlantic. In *Reporters Committee*, the Supreme Court applied a test similar to the one applied by the ECJ in order to answer the question of whether "rap sheets" compiled by the FBI were subject to disclosure upon a request made pursuant to the Freedom of Information Act ("FOIA").[310] The Court opined that "the fact that an event is not wholly "private" does not mean that an individual has no interests in limiting disclosure or dissemination of the information,"[311] and

---

[307] Advanced Web Ranking has released a study showing fresh data on the click-through-rate from Google's organic search results. The data was taken from Google Webmaster Tools Search Queries reports from large accounts back in July 2014. On average, 71.33% of searches resulted in a page one Google organic click. Pages two and three get only 5.59% of the clicks. On the first page alone, the first five results account for 67.60% of all the clicks and results six to ten account for only 3.73%. *See* Philip Petrescu, *Google Organic CTR—2014 Report*, ADVANCED WEB RANKING BLOG (Apr. 15, 2019), www.advancedwebranking.com/blog/google-organic-ctr/ [https://perma.cc/2U28-UCYK].

[308] Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1535 (2012).

[309] Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, ¶ 81.

[310] *See* Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 772 (1989).

[311] *Id*. at 770 (quoting William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, KAN. L. SCH. pt. 1, p. 13 (Sept. 26, 1974)).

determined that "whether disclosure of a private document under the Freedom of Information Act [("FOIA")] Exemption 7(C) is warranted must turn on the nature of the requested document."[312] In this case, the Court concluded that "[t]he privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age eighty, when the FBI's rap sheets are discarded."[313]

Keeping in mind the results the European courts reached in various cases, it is clear that, at the EU level, there is no possible pre-determined hierarchy between the protection of private life and that of freedom of expression. Both rights are worthy of equal respect, and it is impossible to draw a bright line between privacy/data protection and the public's right to know.[314] Indeed, as it can be seen in several judgments rendered before *Google Spain* as well, on the basis of Articles 7 and 8 of the EU Charter of the Fundamental Rights, neither the right to erase nor the right to freedom of expression is absolute.[315] The exercise of both rights depends on many variables and each request will have to be evaluated individually.[316] This phenomenon leads some commentators to

---

312 *Id*. at 750.

313 *Id*. at 771.

314 Stefan Kulk & Frederik Zuiderveen Borgesius, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 320 (Jules Polonetsky & Omer Tene & Evan Selinger eds., 2018), https://pure.uva.nl/ws/files/9113768/Kulk_Zuiderveen_Borgesius_RTBF_chapter_2Feb2017.pdf [https://perma.cc/7DUK-EQ9P].

315 Case C-92/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, ¶ 48; Case C-543/09, Deutsche Telekom AG v. Bundesrepublik Deutschland, 2011 E.C.R. 279, ¶ 51, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0543 [https://perma.cc/2BXJ-VB7C]; Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 E.C.R. 401, ¶ 33, http://curia.europa.eu/juris/celex.jsf?celex=62012CC0291&lang1=en&type=TXT&ancre= [https://perma.cc/5KLM-QWL2].

316 Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, ¶ 81 ("[I]nasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights.").

think that the conditions to exercise these rights are vague in the EU.[317]

However, one thing is clear: in the EU, individuals are entitled to choose which aspects of their personal lives should be private and protected against outside interferences, unless compelling reasons justify restricting that right in certain areas of life or in specific situations.[318] Searching for the name of a specific individual "enables any Internet user to obtain through the list of results a structured overview of the information . . . that can be found on the Internet . . . and which, without the search engine, could not have been interconnected or could have been only with great difficulty—and thereby to establish a more or less detailed profile."[319] In other words, the search engine plays a crucial role in the dissemination of information, and search service providers have an economic interest in such activity.[320] The ECJ ruled that, neither the search service provider's interest in profit-making nor the public's hypothetical interest in outdated and irrelevant information—disclosure of which is facilitated by the search engine—can be deemed a good enough reason to interfere with individual self-determination.[321]

Nevertheless, as the Court of Amsterdam stated in a case where it was asked to apply the *Google Spain* ruling, that rule "does not intend to protect individuals against all negative communications on

---

317 *See* Miquel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 VAND. J. ENT. & TECH. L. 560 (2016).

318 *See* ECHR, *supra* note 55, art. 8 ("Right to Respect for Private and Family Life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.")

319 Case C-131/12, Google Spain SL, at ¶ 80.

320 For some, this means that search engines inevitably influencing the results they display to individuals can be held responsible for selecting the information that is made available to Internet users. In this vein, see Aleksandra Kuczerawy & Jef Ausloos, *NoC Online Intermediaries Case Studies Series: European Union and Google Spain*, INTERDISC. CTR FOR L. & ICT (ICRI), KU LEUVEN 22 (2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567183 [https://perma.cc/V9WN-L98M].

321 Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, ¶¶ 81, 99.

the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions."[322] *Manni* is a good example of this limitation. In this case, the ECJ ruled that, unlike the service offered by Google, the service of a public register providing official and objective information about the situation of a business cannot be considered intrusive into private life.[323]

This decision should not be seen as contradicting *Google Spain*. Although the categorical distinction between things private and things public has been more recently developed and less clearly formulated in American law than it has been in continental legal traditions,[324] everyone in both jurisdictions is entitled to access to official records,[325] albeit subject to certain limitations, and this right of access is seen as one of the fundamental elements of a representative form of government.[326] *Manni* reflects this policy. A business

---

[322] ECLI:NL:RBAMS:2014:6118, 18 Sept. 2014, C/13/569654 / KG ZA 14–960, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118 [https://perma.cc/WD3G-7QM7]. For a comment, see Joran Spauwen & Jens van den Brink, *Dutch Google Spain Ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals*, INFORRM'S BLOG (Sept. 27, 2014), https://inforrm.org/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/ [https://perma.cc/PMF3-JKU].

[323] Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, ¶ 43.

[324] Chaim Saiman, *Public Law, Private Law, and Legal Science*, 56 AM. J. COMP. L. 691, 692 (2009) ("Despite more than a century of critique and deconstruction, the distinction between private and public law continues to influence the structure of legal thought in the civil law world, and of late, these categories have even migrated to common law systems.").

[325] It nevertheless is true that, in Europe, the distinction is getting blurred in practice. *See* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY 27 (Thomas Burger trans., with the assistance of Frederick Lawrence, 1989).

[326] *See* TEX. GOV'T CODE § 552.000(a) (West 2019) ("Under the fundamental philosophy of the American constitutional form of representative government that adheres to the principle that government is the servant and not the master of the people, it is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may retain control over the instruments they have created. The provisions of this chapter shall be liberally

owner, whose business is registered with the public company register, normally has no reasonable expectation of confidentiality in respect of that business's financial records.[327]

2. Statistical Inference

Approximately 5.5 billion searches are conducted each day with Google's search engine.[328] According to the Transparency Report, which Google publishes each year, the company received 800,000 requests between May 2014 and May 2019 from EU citizens wishing to remove links to personal information from its index, which would entail deleting approximately three million URLs.[329] Even if, at first sight, the number of such requests (an average of 600,000 per year) seems high, the impact of delisting on the free speech of citizens is extremely limited. Google assesses each request on a case-by-case basis. It is not compelled to accept all requests, and does not do so. Arguably, "Google is a biased party, as its failure to comply with the ruling leaves one percent of its global revenues at stake[,] . . . [which creates] strong incentives to overreach and remove links that do not deserve to be taken down."[330]

What is sure is that this regime favoring self-regulation permits the search engine company to operate as a private administrative

---

construed to implement this policy."); *see also* ALAN CHARLES RAUL, PRIVACY AND THE DIGITAL STATE: BALANCING PUBLIC INFORMATION AND PERSONAL PRIVACY 37 (2002).

[327] In the United States, some states like Delaware permit a limited liability company (LLC) to be set up without providing state officials the name of the members and managers. *See, e.g.*, 6 DEL. CODE § 18–305 (2015). LLCs are required to include their own ownership information with tax filings. However, those documents are not public. Indeed, IRC Section 6103 generally protects tax return information from disclosure to other parties by an IRS employee. *See Disclosure Laws*, IRS, https://www.irs.gov/government-entities/federal-state-local-governments/disclosure-laws [https://perma.cc/D2PB-MTF9].

[328] *Google Annual Search Statistics*, STAT. BRAIN RES. INST., https://www.statisticbrain.com/google-searches/ [https://perma.cc/FVM2-CLP7]; *see also* Danny Sullivan, *Google Now Handles at Least 2 Trillion Searches Per Year*, SEARCH ENGINE LAND (May 24, 2016, 12:00 PM), https://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247 [https://perma.cc/R28G-QZXM].

[329] *Transparency Report: Search Removals Under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview?hl=en [https://perma.cc/84UX-LR5A].

[330] Steven M. LoCascio, *Forcing Europe to Wear the Rose-Colored Google Glass: The "Right to Be Forgotten" and the Struggle to Manage Compliance Post*, 54 COLUM. J. TRANSNAT'L L. 297, 329 (2015).

agency,[331] which in effect administers public rights on the basis of factors such as the existence of alternative solutions, technical reasons, or duplicate URLs.[332] The newsworthiness of the information from a public interest point of view also plays a role in the company's decision making on removal requests.[333] According to Google's presentation of the results of this evaluation process in a transparency report,[334] the search engine company refused to remove URLs in 55.6% of the cases between May 2014 and May 2019.[335] This means that the average number of the pages actually removed per year is only slightly more than 250,000. Google has accepted all of the removal requests in those cases (14.2% of the total requests) where no reference to the requester's name can be found in the content page at the provided URL, even though the individual's name appears in the URL.[336] When we subtract these 35,500 cases which have absolutely no impact on free speech from the total number of pages that were removed, the number of the removed pages whose content includes the requester's name gets even smaller: about 215,000 pages per year.

Ultimately, the number of removed pages mentioned above corresponds to one very small fraction of the total pages indexed by

---

331 Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1072 (2016).

332 The power given to the search engine to determine which links should be erased has been criticized on different bases. A commentator wrote that "[this] is reinforcing the dangerous trend toward privatized online censorship." *See* Félix Tréguer, *Right to Be Forgotten: With Free Expression Under Threat, Europe Needs a 'Marco Civil Moment*,*'* GLOBAL VOICES (Nov. 9, 2014, 5:45 PM), https://globalvoices.org/2014/09/11/right-to-be-forgotten-with-free-expression-under-threat-europe-needs-a-marco-civil-moment/ [https://perma.cc/DKR3-TWBW]. Another commentator wrote that "the [ECJ] was less clear about how Google, or other search engines, should determine which removal requests to honor." Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L.J. 297, 314 (2018).

333 *See Transparency Report*, *supra* note 329.

334 In May 2015, eighty academics addressed a letter to Google, asking for more transparency about its evaluation processes. *See* Ellen P. Goodman, *Open Letter to Google from 80 Internet Scholars: Release RTBF Compliance Data*, MEDIUM (May 13, 2015), https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd [https://perma.cc/B4J7-MFYB].

335 *Transparency Report*, *supra* note 329.

336 *Id*.

Google, which exceeded 130 trillion pages in 2016.[337] The removed links represent less than 0.0000002% of the pages to which Google offers access. This number is so small that it is hard to believe that the ECJ's ruling has "foray[ed] into the significance of communication on the Internet,"[338] or "unearth[ed] a myriad of global media law issues,"[339] or "effectuat[ed] international censorship in the guise of privacy."[340] On the contrary, the figures mentioned above demonstrate that, in the EU, the right to privacy coexists with the right to information and with freedom of expression. The case law of the ECJ restricts the exercise of the right to erase in circumstances, where the dissemination of information about an individual constitutes an intrusion into a private matter without sufficient countervailing public benefits.[341]

If we believe, like many commentators, that the removal of a number smaller than 0.0000002% of all the indexed pages is large enough to infringe freedom of information or freedom of expression, we should also file complaints against the companies, public authorities, and website operators gathering and disclosing information for missing links or websites which cover matters being of public interest. Indeed, 85% of content disappears within a year and 59% within a week for a number of reasons[342]: websites are refreshed every couple of years to keep current with advancements, companies are taken over or go out of business, websites are blocked by

---

337 In November 2016, Google mentioned in the "How Google Search Works" page that it had indexed 130 trillion pages. That figure is up by 100 trillion pages from when Google announced 30 trillion pages in March 2013. The company has not shared any newer number. Taking into account the increase of 333% from 2013 to 2016, the number of indexed pages should be much more than 130 trillion pages today. *See How Google Search Works, Crawling & Indexing*, GOOGLE, www.google.com/search/howsearchworks/crawling-indexing/ [https://perma.cc/FT2V-YVTZ].

338 Post, *supra* note 35, at 1071.

339 BYRUM, *supra* note 36, at xiii.

340 McKay Cunningham, *Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, 69 ARK. L. REV. 71, 114 (2016).

341 Case C-131/12, Google Spain v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317, ¶ 81; Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, ¶¶ 47, 64, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

342 Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten*, 16 STAN. TECH. L.J. 101, 101 (2013).

governments or by ISPs, shut down by copy-right holders enforcing their rights, or sometimes links get broken,[343] content gets overwritten for technical reasons even before information is archived.[344]

The number of broken or lost web pages is much higher than that of deliberately removed web pages containing personal data. Oceans of scholarly ink have been spilled on the "inappropriateness" of *Google Spain*, whose impact is much less important.[345] Yet, curiously, there is very little—perhaps no—popular reaction indicating that this "lost content" prevents people from developing the "public opinion that is essential to a democracy."[346]

Data privacy issues are not limited to the public disclosure of embarrassing private facts. There are other types of breaches which undermine the authority of the individual to decide herself or himself, on the basis of the idea of self-determination, when and within what limits information about her or his private life should be communicated to others.[347] Some numbers recently cited by the

---

[343] The average website lifespan is two years and seven months. *See* Andy Crestodina, *What Is the Average Website Lifespan? 10 Factors in Website Life Expectancy*, ORBIT MEDIA STUDIOS, www.orbitmedia.com/blog/website-lifespan-and-you/ [https://perma.cc/RH5R-PCVQ].

[344] PAUL BERNAL, THE INTERNET, WARTS AND ALL: FREE SPEECH PRIVACY AND TRUTH 30 (2018).

[345] *See*, *e.g.*, Wilbur Ross, *EU Data Privacy Laws Are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018, 12:42 PM), www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c; Bromund, *supra* note 37; BYRUM, *supra* note 36, at 111–12 (2018); *see generally* David Erdos, *European Union Data Protection Law and Media Expression: Fundamentally Off Balance*, 65 INT'L COMP. L.Q. 139 (2016); Emily Adams Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulat*ion, 39 BROOK. J. INT'L L. 487 (2014); Patricia Sánchez Abril & Jacqueline D. Lipton, *The Right to Be Forgotten: Who Decides What the World Forgets*, 103 KY. L.J. 363487 (2014); Sophie Curtis & Alice Philipson, *Wikipedia Founder: EU's Right to Be Forgotten Is "Deeply Immoral*," TELEGRAPH (Aug. 6, 2014, 12:07 PM), www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html [https://perma.cc/PSM9-L795]; LoCascio, *supra* note 330; Bromund, *supra* note 37.

[346] Post, *supra* note 35, at 1042.

[347] Personal information can contain financial information such as credit card information, the disclosure of which can cause financial loss to the user. It can also contain other information such as political affiliation or medical records, the disclosure of which can result in non-financial loss such as injury to feelings. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 888–89 (2014). In the United States, the definition of

CPO (Chief Privacy Officer) Magazine give an idea about the magnitude of the major data breaches so far[348]:

Company	Accounts Hacked	Date of Hack
Yahoo!	3 billion	Aug. 2013
Marriott	500 million	2014–2018
Yahoo!	500 million	Late 2014
Adult FriendFinder	412 million	Oct. 2016
MySpace	360 million	May 2016
Under Armor	150 million	Feb. 2018
Equifax	145.5 million	July 2017
Ebay	145 million	May 2014
Target	110 million	Nov. 2013
Heartland Payment Systems	100+ million	May 2008
LinkedIn	100 million	June 2012
Rambler.ru	98 million	Feb. 2012
TJX	94 million	2003–2004
AOL	92 million	2004

personal information varies by the specific jurisdiction and law. In the EU, Article 4(1) of the GDPR defines "personal data" very broadly as "any information relating to an identified or identifiable natural person ('data subject')." GDPR, *supra* note 17, art. 4(1).

348 Matt Powell, *11 Eye Opening Cyber Security Statistics for 2019*, CPO MAG. (June 25, 2019), www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/ [https://perma.cc/7T6M-7TRN].

Company	Accounts Hacked	Date of Hack
MyHeritage	92 million	Oct. 2017
Sony PlayStation Network	77 million	Apr. 2011
JP Morgan Chase	83 million	July 2014
Tumblr	65 million	Feb. 2013
Uber	57 million	Late 2016
Home Depot	53 million	Apr. 2014
Facebook	50 million	July 2017

Taking into account the total number of people using the services provided by each of the companies listed above (e.g. Uber has around 75 million users),[349] the number of hacked accounts corresponds to a significant proportion of the users (e.g. 57 million for Uber) and thus represents a grave problem. For all of these service companies, the proportion of the number of victims of mass data hacks (e.g. 76% for Uber) is considerably higher than the 0.0000002% of pages actually deleted as a result of *Google Spain*. This disparity suggests that the real issue in the context of data privacy is the data consent policies which do not give users enough control over the way their information is collected and processed, and ultimately the mass violation of personal autonomy, rather than the violation of freedom of expression and the implications of the right to be de-indexed.

B. Practical Concerns and Approaches in the United States

In the United States, one of the most common arguments courts rely on to dismiss invasion of privacy claims arising from data breaches is the absence of sufficient evidence proving direct or

---

[349] *See Uber by the Numbers: Users & Drivers Statistics, Demographics, and Fun Facts*, MUCH NEEDED, https://muchneeded.com/uber-statistics/ [https://perma.cc/FH7E-GVJ8].

actual harm,[350] since most data breach cases are based solely on speculative future harm.[351]

In *In re U.S. Office of Personnel Management Data Security Breach Litigation* ("AFGE v. OPM"), where lawsuits were filed on the basis of the Privacy Act of 1974 against the Office of Personnel Management ("OPM") over data breaches compromising the records of 22 million federal employees, the U.S. District Court for the District of Columbia acknowledged the "troubling allegations" raised by OPM's victims.[352] Nevertheless, the court ruled that "the fact that a person's data was taken [is not] enough by itself to create standing to sue."[353] In *In re Science Applications International Corp.*, the same court stated that "the degree by which the risk of harm has increased is irrelevant [to standing]—instead, the question is whether the harm is certainly impending."[354]

In spite of a general tendency to support disclosure, American courts, just like European courts, have nevertheless consistently protected personal information—or the "intimate details of one's private life"—whose release could cause the individual personal distress or embarrassment.[355] For instance, on June 21, 2019, the U.S. Court of Appeals for the District of Columbia reversed the district court's order in *AFGE v. OPM* granting dismissal of the complaints discussed above, holding that the plaintiffs' allegations of potential "future harm" were sufficient for the case to move forward.[356]

---

350 Aranda v. Caribbean Cruise Line, Inc., 202 F. Supp. 3d 850, 855–56 (N.D. Ill. 2016) (citing Smith v. Ohio State Univ., 191 F. Supp. 3d 750 (S.D. Ohio 2016); Gubala v. Time Warner Cable, Inc., No. 15-cv-1078-pp, 2016 WL 3390415, at *1 (E.D. Wisc. June 17, 2016); Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524 (D. Md. 2016).

351 *Khan*, 188 F. Supp. 3d, at 529.

352 *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 9 (D.D.C. 2017).

353 *Id*. at 9. The court reasoned that it was "constrained to find that plaintiffs cannot predicate standing on the basis of the breach alone." *Id.* at 20.

354 *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014).

355 Personal information was described by the California Court of Appeal as the "intimate details of one's private life." Wasser v. San Diego Union, 191 Cal. App. 3d 1455, 1460 (1987).

356 *In re* United States Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 59 (D.C. Cir. 2019).

The decisions American courts have made can be divided in two main categories: (1) collection and use of private information by government agencies on the basis of the Fourth Amendment, the FOIA,[357] and the Privacy Act of 1974[358]; and (2) collection and use of private information by private individuals. A simultaneous analysis of both categories will produce a global picture of the practical concerns and approaches of American courts that reveals them to be remarkably similar to the concerns and approaches of the ECJ.

First, I will focus on the balance between access to public records by government agencies and the privacy rights of the individuals whose personal information is in those records. As in Europe, there is a widespread understanding in the United States that the "open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."[359] According to a paper published by the Center for Democracy and Technology, public records in the United States include driver's license, driving records, motor vehicle registration, land titles, property tax records, voting registration records, occupational licenses, use licenses (e.g. ham radio, CB radio), firearm permits, court records, bankruptcy filings, civil actions, criminal histories, divorces, docket information, juror information, wills, law enforcement records, police blotters, jail lists, compiled criminal history records, political contributions, securities and exchange commission filings, financial disclosure filings, hunting and fishing licenses, boat, aircraft and other vehicle titles, and U.S. postal service address records.[360]

While providing a broad right of access to these documents in the possession of the executive branch of the federal government, the FOIA serves as the vehicle for discovering and reporting numerous matters of public interest. Although no specific EU law

---

357 *See* 5 U.S.C. § 552 (2018).

358 *See id.* § 552a.

359 FRED H. CATE & RICHARD J. VARN, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS: A NEW FRAMEWORK FOR FINDING THE BALANCE 1, 5 (1999), *available at* https://it.ojp.gov/documents/d/Public_Record.pdf [https://perma.cc/VN2G-UL84].

360 Robert Gellman, *Public Records—Access, Privacy and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q. 391, 392 (1995).

resembles the FOIA, *Manni* makes clear that the compilation of a public register providing official data about an objective situation cannot, except in specific circumstances, be deemed intrusive into private life.[361] Thus the ECJ's case law shows that the Court's approach resembles that of the FOIA.

According to the ECJ's ruling, even after a sufficiently long period of time has elapsed since the specific case in question, only a few, overriding reasons justify limiting third party access to personal data.[362] The FOIA creates exemptions that address the need for privacy, in a way similar to the *Manni* ruling, and finds a middle ground.[363] The justification of this limitation lies in the need for certain files held by the federal government, which contain information personal enough in nature that its disclosure would very likely constitute an "unwarranted invasion of personal privacy," to be protected against disclosure.[364] Public access to official records is thus a conditional right in both the United States and in the EU.

A few decisions handed down by American courts reflect the tensions and complexities regarding the public's interest in both access to public records and personal privacy. In *Associated Press*, the Court of Appeals for the Second Circuit decided, on the basis of FOIA Exemption 6, that Guantanamo Bay detainees and their family members have a "measurable privacy interest" in the nondisclosure of their names and identifying information contained in records regarding allegations of abuse by military personnel and other detainees.[365] The Court highlighted that "a detainee might want to voluntarily disclose information publicly does not authorize the government to disclose that information."[366]

---

361 Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, ¶ 63, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

362 *Id*. at ¶ 60.

363 *See* Martin E. Halstuk & Bill F. Chamberlin, *The Freedom of Information Act 1966–2006: A Retrospective on the Rise of Privacy Protection over the Public Interest in Knowing What the Government's Up to*, 11 COMM. L. & POL'Y 511, 511 (2006).

364 5 U.S.C. § 552(b)(6) (2016).

365 Associated Press v. U.S. Dep't of Def., 554 F.3d 274, 274–79 (2d Cir. 2009).

366 *Id*. at 287.

According to the U.S. Justice Department, courts regularly rule against the disclosure of sensitive personal information regarding marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, social security numbers, criminal history records, incarceration of U.S. citizens in foreign prisons, sexual inclinations or associations, and financial status.[367] With regard to financial status, even though corporations have no privacy rights, personal financial information is nevertheless protected—particularly information concerning small businesses when the individual and corporation are identical.[368] In *Veneman*, a Texan court ruled that the Department of Agriculture had incorrectly considered individuals participating in a USDA program as "businesses" because of their ownership of a certain number of livestock or because of the fact that their ranch had a name.[369] The court concluded that personally identifying information about those individuals should not be disclosed.[370]

Disclosing lists of names, telephone numbers, and email addresses of individuals has frequently been the reason behind privacy litigation.[371] Courts have in effect established a non-official nondisclosure rule regarding the public release of mailing lists. The D.C. Circuit, for instance, ruled that mailing lists with the names and home addresses of federal annuitants were categorically nondisclosable under FOIA's privacy exemption.[372] The Supreme Court

---

[367] *See* U.S. DEP'T OF JUST., GUIDE TO THE FREEDOM OF INFORMATION ACT, EXEMPTION 6, 480 (2014), *available at* https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6_0.pdf [https://perma.cc/W65B-2LMY].

[368] *See, e.g.*, Providence Journal Co. v. Fed. Bureau of Investigation, 460 F. Supp. 778, 785 (D.R.I. 1978), *rev'd on other grounds*, 602 F.2d 1010 (1st Cir. 1979); Beard v. Espy, No. 94-16748, 1995 WL 792071, at *1 (9th Cir. Dec. 11, 1995); Nat'l Parks & Conservation Ass'n v. Kleppe, 547 F.2d 673, 685–86 (D.C. Cir. 1976); Okla. Publ'g Co. v. HUD, No. Civ-87-1935-P, 1988 U.S. Dist. LEXIS 18643, at *4–5 (W.D. Okla. June 17, 1988); DEP'T OF JUST., FOIA UPDATE, VOL. III, NO. 4, 5 (1982), https://www.justice.gov/oip/blog/foia-update-foia-counselor-questions-answers-24 [https://perma.cc/EZ6M-DRKG].

[369] Doe v. Veneman, 230 F. Supp. 2d 739, 750 (W.D. Tex. 2002), *aff'd in pertinent part on other grounds*, 380 F.3d 807, 818 (5th Cir. 2004).

[370] *Id*. at 749–51, 807.

[371] *See, e.g.*, *supra* notes 7–14 and accompanying text.

[372] *See* Nat'l Ass'n of Retired Fed. Employees v. Horner, 879 F.2d 873, 879 (D.C. Cir. 1989).

also specifically considered the issue, and held that compilations of names and home addresses of private citizens are protected under the privacy exemption,[373] although this is not the case for corporations.[374] Moreover, the Supreme Court's Fourth Amendment jurisprudence has recognized the intrusiveness of observing personal cell phone data. In *Riley*, the Court stated that the warrantless search of the data contained on a cell phone may be even more intrusive than the search of a home.[375] In his reasoning, Chief Justice John Roberts acknowledged the high value of protecting private digital information in the search and seizure and public safety realm.[376] The Supreme Court took privacy protection a step further in *Carpenter*.[377] In this landmark case, the Court ruled that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured" through cell phone location data, and that "the Government must generally obtain a warrant supported by probable cause before acquiring such records."[378]

These decisions demonstrate that, in the evaluation criteria determining whether private data collected by government agencies should be made publicly available, American courts are not indifferent to the nature of the information in question, its sensitivity for the data subject's private life, the data subject's identity, the purpose of its storage and disclosure, and the public's concern or interest in the information. The approach of American courts in the evaluation of the collection and use of information by private individuals or non-governmental entities likewise is to examine fundamental rights and other relevant interests on a case-by-case basis. Particularly the seminal 2001 case *Bartnicki*, which has set off

---

373 *See* U.S. DEP'T OF JUST., FREEDOM OF INFORMATION ACT GUIDE (2004), https://www.justice.gov/oip/foia-guide-2004-edition-exemption-6#exemption [https://perma.cc/25NM-NT5Q]; *see also* Bibles v. Oregon Natural Dessert Ass'n, 519 U.S. 355 (1997); U.S. Dep't of Def. v. Fed. Labor Relations Auth., 114 S. Ct. 1006 (1994).

374 In *Dep't of Justice v. Reporters Committee for Freedom of the Press*, the Court denied the personal privacy FOIA exemption to corporations. 489 U.S. 749, 749 (1989). For more on this case, see generally Patrick C. File, *A History of Practical Obscurity: Clarifying and Contemplating the Twentieth Century Roots of a Digital Age Concept of Privacy*, 6 U. BALT. J. MEDIA L. & ETHICS 4 (2017).

375 Riley v. California, 134 S. Ct. 2473, 2491 (2014).

376 *Id*. at 2494–95.

377 *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

378 *Id*. at 2217, 2221.

a wrenching debate over the privacy values society is actually willing to protect, illustrates well the Supreme Court's approach to the publication of data breaches.[379] While the case is not very recent, its principles still apply today. Moreover, the holding of the Court is flexible enough to deal with technological advances in communications and media research.[380]

In *Bartnicki*, the Court analyzed the constitutionality of restrictions on publishing information[381] illegally obtained through the interception of phone conversations.[382] The Court set forth a three-prong balancing test that examines the conduct of the defendant, the nature of the disclosure, and the importance of the disclosure for the public interest. According to the Court, matters of public concern or interest are newsworthy matters that relate to current events.[383] From the point of view of this Article, this raises the question as to whether search engine companies have the right in the United States to facilitate the publication and dissemination of personal information that does not deal with current, newsworthy subjects.[384]

Financial records, such as social security debts (as in *Google Spain*), cannot be considered newsworthy.[385] The main reason

---

379 *See* Bartnicki v. Vopper, 121 S. Ct. 1753 (2001).

380 Richard D. Shoop, Bartnicki v. Vopper, 17 BERKELEY TECH. L.J. 449, 461 (2002).

381 *Bartnicki*, 121 S. Ct. at 1756. For similar cases, see, e.g., Boehner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999), *cert. granted*, 532 U.S. 1050, 121 S. Ct. 2190; Peavy v. WFAA-TV, Inc*.,* 37 F. Supp. 2d 495 (N.D. Tex. 1999), *aff'd in part, rev'd in part,* 221 F.3d 158 (5th Cir. 2000). *See also* Eric Easton, *Ten Years After:* Bartnicki v. Vopper *as Laboratory for First Amendment Advocacy and Analysis*, 50 U. LOUISVILLE L. REV. 287, 294 (2011).

382 *See* 18 U.S.C. § 2511(1) (2012) (stating that "[e]xcept as otherwise specifically provided in this chapter any person who . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished . . . .").

383 *See Bartnicki*, 121 S. Ct. at 1760; *see also* New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

384 *Bartnicki*, 121 S. Ct. at 1760.

385 *See, e.g.*, Painting and Drywall Work Pres. Fund v. Dep't of Hous. & Urban Dev., 936 F.2d 1300, 1303 (D.C. Cir. 1991); Hopkins v. U.S. Dep't of Hous. & Urban Dev., 929 F.2d 81, 87 (2d Cir. 1991); Robyn v. Phillips Petroleum Co., 774 F. Supp. 587, 592 (D. Colo. 1991); Adams v. Murakami, 813 P.2d 1348, 1365 (Cal. 1991) (Mosk, J., dissenting); Doyle v. State Bar, 648 P.2d 942, 945 (Cal. 1982); Valley Bank of Nev. v. Superior Court, 15

behind the Supreme Court granting Congress permission to restrict the speech of consumer reporting agencies and financial institutions is that consumer reports and private financial records are confidential and cannot be deemed to be newsworthy,[386] since, in ordinary circumstances, this type of information can be described as the "intimate details of one's private life."[387] Besides financial records,[388] due to their confidentiality, other types of sensitive personal information, such as medical conditions, religious affiliations, and sexual inclinations or associations are accessible only to authorized parties that need the information for permissible purposes (e.g., employment purposes, credit transactions, or insurance underwriting).[389] The requirement of permissible purposes constitutes a precaution to stop unauthorized third parties from disclosing personal information that is not newsworthy or has become obsolete.[390]

The judicial approach just described is similar to that taken by the ECJ in *Google Spain*, where the Court required the search engine company to delist personal information as long as the information is "no longer relevant" or, in the words of the U.S. Supreme Court in *Bartnicki*, no longer newsworthy.[391] An unflattering old piece of news, for instance, is less newsworthy than new information, as in general it lacks public interest. As the Supreme Court of California highlighted in *Shulman*, even an individual unwillingly involved in a newsworthy incident does not surrender all rights to privacy, and not everything said or done by that person is newsworthy[392]:

Cal.3d 652, 656 (Cal. 1975); City of Carmel-by-the-Sea v. Young, 466 P.2d 225, 231 (Cal. 1970); Terry York Imports, Inc. v. Dep't of Motor Vehicles, 242 Cal. Rptr. 790, 797 (Cal. Ct. App. 1987); Tollefson v. Price, 430 P.2d 990, 992 (Ore. 1967); Palmisano v. Toth, 624 A.2d 314, 318–19 (R.I. 1993).

386 *See supra* note 385; *see generally* United States v. Bormes, 133. S. Ct. 12 (2012); Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011); Watters v. Wachovia Bank, N.A., 550 U.S. 1 (2007).

387 Wasser v. San Diego Union, 236 Cal. Rptr. 772, 775 (1987).

388 *See, e.g.*, 15 U.S.C. § 1681(b).

389 *See* U.S. DEP'T OF JUST., *supra* note 367, at 480.

390 *See* SOLOVE & SCHWARTZ, *supra* note 202, at 750–51 (5th ed. 2014).

391 Bartnicki v. Vopper, 121 S. Ct. 1753, 1776 (2001).

392 *See* Shulman v. Group W Productions, Inc. 955 P.2d 469 (Cal. 1998); *see also* Gary L. Bostwick, *The Newsworthiness Element: Shulman v. Group W. Prods., Inc. Muddies the Waters*, 19 LOY. L.A. ENT. L. REV. 225, 239–40 (1999).

> First, the analysis of newsworthiness does involve courts to some degree in a normative assessment of the 'social value' of a publication. . . . All material that might attract readers or viewers is not, simply by virtue of its attractiveness, of *legitimate* public interest. Second, the evaluation of newsworthiness depends on the degree of intrusion and the extent to which the plaintiff played an important role in public events . . . , and thus on a comparison between the information revealed and the nature of the activity or event that brought the plaintiff to public attention.[393]

Another point that the *Bartnicki* Court highlighted is the fact that the First Amendment protection is not absolute, but rather is conditioned upon whether personal information is obtained through proper means (e.g., via a permissible purpose or express consent) or in an unlawful way.[394] The Court decided that broadcasting the stolen audio recording in question benefited from the protection offered by the First Amendment on account of the public importance of the recording, and on account of the fact that the defendant was not responsible for the initial breach although he was aware the recording had been obtained illegally.[395] The Court specified it would consider punishing disclosure should the disclosing party have engaged in illegal activity to procure the information.[396] Indeed, as Dean Post pointed out, "the First Amendment has traditionally been dedicated to the creation of free public opinion, not to the creation of public knowledge."[397] In *Dahlstrom*, the Court of Appeals for the Seventh Circuit used the *Bartnicki* three-part test to determine that the First Amendment did not protect the Chicago Sun Times from liability for publishing personal information about five police officers that it had illegally obtained from government records and published without permission, because the information was not of sufficiently high public interest.[398] The Court highlighted

---

393 *Shulman,* 955 P.2d at 483–84 (citations omitted).
394 *See Bartnicki*, 121 S. Ct. at 1760, 1764.
395 *See id*.
396 *See id*. at 1762.
397 Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 487 (2011).
398 Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 940–41, 954 (7th Cir. 2015).

the Supreme Court's holding in *Branzburg*[399] that the First Amendment "does not guarantee the press a constitutional right of special access to information not available to the public generally."[400]

In respect of privacy and free communication, the social norms and values embodied in the United States law do not substantially differ from those of the EU law. Courts on both sides of the Atlantic are reluctant to accept a possible pre-determined hierarchy between data protection and the free flow of information in society. Data protection does not automatically override freedom of the press and freedom of expression or *vice versa*.[401] Decisions are based on an issue-by-issue examination of different fundamental rights, and other interests.[402]

In addition to practical solutions, some procedural principles and applications in terms of access to justice once data has been allegedly misused, too, are similar on both sides of the Atlantic. Influenced by the U.S. model, Article 80, section 1 of the GDPR gives individuals the right to bring a collective legal action in case of intrusion of privacy, an innovative type of action for the continental European legal tradition.[403] Although the new European

---

399 *Id.* at 946 (citing Branzburg v. Hayes*,* 92 S. Ct. 2646 (1972)).

400 *Branzburg*, 92 S. Ct. at 2658.

401 In the United States, see Zacchini v. Scripps-Howard Broad. Co., 97 S. Ct. 2849 (1977) (pointing out the limits the First Amendment places on the right of entertainers to control public dissemination of their performances, and ruling for the entertainer stating that the First Amendment does not give the broadcaster the right to appropriate the entertainer's entire act). In the EU, see Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E.C.R. 317; Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2016 E.C.R. 652, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183142&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3853759 [https://perma.cc/8Z25-NB83].

402 In the United States, see, e.g., Bartnicki v. Vopper, 121 S. Ct. 1753, 1753 (2001). In the EU, see, e.g., Case C-92/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, ¶ 48; Case C-543/09, Deutsche Telekom AG v. Bundesrepublik Deutschland, 2011 E.C.R. 279 ¶ 51, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0543 [https://perma.cc/2BXJ-VB7C]; Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 E.C.R. 401 ¶ 33, http://curia.europa.eu/juris/celex.jsf?celex=62012CC0291&lang1=en&type=TXT&ancre= [https://perma.cc/XPT8-3VPL].

403 GDPR, *supra* note 17, art. 80 ("The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms

opt-in collective action falls short of the American opt-out class action right, it can be viewed as a first move towards increasing the number of group privacy claims in Europe. By establishing in the GDPR collective redress methods, the EU legislature has taken an important step forward in permitting consumers and members of labor unions to come together as a group, assert their privacy rights, and seek redress by way of claiming compensation.[404]

While the EU legislature seems willing to expand collective action on the basis of a model seeking to avoid the kind of frivolous suits that many Europeans—with or without basis—associate with American class action practice,[405] it is noteworthy that similar concerns have arisen within the United States.[406] As Professors Gelbach and Hensler noted, "nearly a decade's worth of U.S. Supreme Court cases have restricted the scope and ease of use of the class action device."[407] Worries regarding potential abuse and misuse of class actions in data protection cases, among others, appear to be motivating legislatures and courts on both sides of the Atlantic to be cautious. This is a significant indicator suggesting that not only their substantive law on data protection, but also their procedural law governing the administration of privacy policies in general have started converging as a result of increased interaction between the legal cultures of the United States and the EU.

---

with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise . . . the right to receive compensation . . . .").

[404] For more on this topic, see generally Laima Jančiūtė, *Data Protection and the Construction of Collective Redress in Europe: Exploring Challenges and Opportunities*, 9(1) INT'L DATA PRIVACY L. 2 (2019).

[405] Commission Recommendation 2013/396/ of 11 June 2013 on Common Principles for Injunctive and Compensatory Collective Redress Mechanisms in The Member States Concerning Violations of Rights Granted Under Union Law, O.J. (L 201) ¶ 10 ("safeguarding against abuse"); ¶ 13 ("prevent abuse"); ¶ 19 ("in such a way that it cannot lead to an abuse of the system"); ¶ 20 ("[i]n order to avoid an abuse of the system"); ¶ 22 ("the need to avoid abuse"). For more information, see generally EVA LEIN, DUNCAN FAIRGRIEVE, MARTA OTERO CRESPO & VINCENT SMITH, COLLECTIVE REDRESS IN EUROPE: WHY AND HOW? 1 (2015).

[406] *See* Deborah R. Hensler & Thomas D. Rowe, Jr., *Beyond "It Just Ain't Worth It": Alternative Strategies for Damage Class Action Reform*, 64 L. & CONTEMP. PROBS. 137 (2001).

[407] Jonah B. Gelbach & Deborah R. Hensler, *What We Don't Know About Class Actions but Hope to Know Soon*, 87 FORDHAM L. REV. 65 (2018).

CONCLUSION

Oscar Wilde was correct when he said that no man is rich enough to buy back his past.[408] One should assume guilt for past wrongdoing, but should also look forward to the future. That is why Wilde's premise must not be understood as implying that personal data should be disclosed without any restriction. I have analyzed the tension that exists on both sides of the Atlantic between the public's right to access information and data privacy. I have paid particular attention to the way recent advances, especially regarding communication technology and social media, have affected:

i) the perceptions of privacy and that of freedom of expression,
ii) the current and prospective reaction of the lawmaker in framing policies that aim at maximizing both interests, and
iii) the standards and tests that courts use to evaluate the dynamics between rights and responsibilities.

I have also asked whether and to what extent there is a similar legislative and judicial evolution in the United States and the EU. My goal has been to demonstrate, from both practical and conceptual perspectives, the dynamic nature of the multitude of variables that influence any decision regarding a possible loss of privacy or restriction of freedom of expression.

My analysis shows that, through *Google Spain* and the adoption of the GDPR, EU law has shaped, to some degree, the evolution of American public policy. In this matter, EU law has perhaps been more influential than American privacy lobbyists. Yet, changes and initiatives at the state as well as national level do not solely result from an apparent economic threat from Europe, but also from a number of concerns regarding data security that have arisen within the United States. Recent statistics illustrate that most people are concerned about the ability of businesses to safeguard their financial and personal information. These concerns, along with several class action lawsuits filed following data leakage or contamination, show

---

408 WILDE, *supra* note 1.

in a roundabout way the inefficiency of the system when it comes to protecting personal information in a satisfactory manner. There is a desire to settle the issue thanks to new legislative measures, instead of relying on the existing legal rules or the case law developing *ad hoc* exceptions to existing rules. One of the reasons for this desire is that the Privacy by Design principles, which require relatively costly implementation processes, have not yet been followed by businesses.

American legislative frameworks, such as the CCPA, that borrow the core principles of the GDPR, are directed toward broadening the scope of data security. These American regimes permit an effective and comprehensive protection, without compromising the promotion of a free, open, and transparent society and market. They grant consumers, among others, a right similar to the right to erase conferred to EU citizens following *Google Spain*. Nevertheless, this legislative entitlement is not an unrestricted right to erase anything that we dislike from the Internet. In fact, figures provided by Google so far show that the number of removed pages is much less important than the number of web pages broken or lost every year, and corresponds to an extremely small percentage (well below 0.0000002%) of all the pages indexed by Google.

On both sides of the Atlantic, the criteria adopted by the legislature in defining the penumbras of (data) privacy in general, and of the right to erase in particular, do not disregard the principles and standards set forth by case law. In the EU, a combined reading of *Google Spain*, *Manni*, and local decisions, such as the one handed down by the Court of Amsterdam, makes it clear that the law protects citizens against outdated or irrelevant links to search results that may intrude on a person's privacy. EU citizens are not entitled to insist that all negative communications about them be removed from the Internet. The nature of the information in question, its sensitivity for the data subject, the data subject's identity (private or corporate), the purpose (profit-making or non-profit public service) of its storage and disclosure, and the public's concern or interest in the information are among the factors that influence the evaluation of the scope of the right to erase personal information. Ultimately, the exercise of the right to erase does not affect the existence of content, but merely the search results.

There is a noticeable parallel between the efforts of American courts and of European courts to find an approach that maximizes both freedom of expression and data security. Rulings such as *Bartnicki*, *Shulman*, *Associated Press*, and *Carpenter* demonstrate that American courts have adopted an ambivalent approach towards data protection. There is no monolithic test that weighs privacy and public interests. Courts weigh various interests, such as the "social value" of a publication and the importance of the role played by the plaintiff in the public events, and in each case the court makes an effort to establish a balance between protecting information that is not newsworthy or of legitimate public concern and broad public access to information that is not acutely personal. In such an evaluation, not only are nature and origin of the information in question significant factors, but so too is the way the information was obtained. The publication of private information, particularly in cases where it is not of public concern or was obtained without consent, leads to similar results on both sides of the Atlantic.

Although American and European legal cultures do assign different meanings to "public concern" and "consent," it would nevertheless be an exaggeration to assert that, as a result of their differences, data privacy law in the United States and the EU offer conflicting solutions. Difference does not automatically imply incompatibility. A deeper analysis of their legislative efforts, case laws, and procedural rules reveal that neither U.S. law nor EU law can be contextualized through a black-and-white approach. On the contrary, the tests, criteria and thresholds used to define data privacy illustrate, on both sides of the Atlantic, the complex and dynamic nature of its assessment. Recent developments show that the principles that underpin such an assessment in the United States and the EU are getting closer. This convergence makes it likely that, in the long run, American and European governmental institutions and courts will reach similar conclusions when they decide privacy or data security cases presenting similar facts.