COMMENT

WHO REALLY CONTROLS THE PRIVACY CONVERSATION? THE NEED FOR A FUNDAMENTAL RIGHT TO PRIVACY IN THE UNITED STATES

ALEXA LYNN WEBER*

CONTENTS

I. INTRODUCTION

A. "Privacy": What Does it Even Mean?

A simple touch of a button allows a person to share one photograph with billions of people.[1] An instant message can easily be sent to a friend sitting across the table, or to a friend across the world.[2] Geographical boundaries cease to exist within the internet. This has transformed the way citizens interact with one another, gather their news, and spend their time. Many people may believe that online privacy has been put on the back burner and ignored, but this comment explores the idea that it is not that simple.[3] As members of society bond over memes or random viral photographs, customers' enjoyment of platforms such as Facebook are guided by differing ideas of what online privacy even means. By analyzing privacy issues through this lens, a better understanding of how the concept of privacy has changed in the digitized world will guide future

* J.D. Candidate, 2021, Sandra Day O'Connor College of Law.

[1] As of December 2019, the internet has approximately 4.54 billion users, while there are 3.725 billion active users on any given social media platform. Kat Smith, *126 Amazing Social Media Statistics and Facts*, BRANDWATCH (Dec. 30, 2019), https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/.

[2] To put this in context, Facebook Messenger and Whatsapp together send out upwards of 60 billion messages in one day. *Id.*

[3] See section II and section III.

discussions.[4] Governments will then be able to enact beneficial legislation for global citizens while still allowing for the free flow of information.[5]

The current privacy policies of companies such as Instagram, Snapchat, or LinkedIn are difficult for lay persons to understand.[6] These policies are not forthcoming and say things such as, "[y]ou should read this in full, but here are a few key things we hope you take away from it."[7] By telling individuals what they need to know, the corporation controls the privacy conversation rather than the individual.[8] For example, Facebook has argued that by posting to one hundred friends on social media, the author of that post has given up privacy interests and has no reasonable expectation of privacy.[9] From a user's perspective, if privacy is defined by the corporation rather than by the individual, it is difficult to trust in those companies to adequately protect privacy interests of users.[10] Rather, the definition of privacy should be defined from an individual perspective because privacy is personal.[11] To illustrate this point, the Chief Executive of Google, Sundar Pichai has stated:

> To the families using the internet through a shared device, privacy might mean privacy from one another. To the small-business owner who wants to start accepting credit card payments, privacy means keeping customer data secure. To the teenage sharing selfies, privacy could mean the ability to delete that data in the future.[12]

There is a disconnect between how much control individuals are willing to take over their privacy and their lack of trust in online corporations. This disconnect stems from a non-existent definition of online privacy with respect to private information, which makes it difficult for legislatures to draft effective privacy regulations for fear of them becoming as convoluted as online

---

[4] See section III.

[5] For a more in-depth discussion of what global citizenship is, see *What is Global Citizenship?*, IDEAS FOR GLOB. CITIZENSHIP, http://www.ideas-forum.org.uk/about-us/global-citizenship (last visited March 1, 2020).

[6] *See, e.g.*, Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource*", 93 S. CAL. L. REV. 99, 100 (2019) (arguing that consumers do not understand the privacy interests they give up by using free resources online and that consumers are unable to read "complicated and lengthy privacy policies").

[7] Twitter, TWITTER PRIVACY POLICY 3 (2020), https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-18th-2020/Twitter_Privacy_Policy_EN.pdf.

[8] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019) ("Additionally, majorities of the public are not confident that corporations are good stewards of the data they collect.").

[9] Facebook argued that sharing on social media platforms "is an affirmative social act to publish, to disclose, to share ostensibly private information . . . .". Charlie Warzel, *Facebook Under Oath: You Have No Expectation of Privacy*, THE N. Y. TIMES (June 18, 2019), https://www.nytimes.com/2019/06/18/opinion/facebook-court-privacy.html (quoting the transcript of proceedings, *In re* Facebook, Inc. Consumer Priv. User Profile Litig., No. 18-MD-02843 (N.D. Cal. June 3, 2019). Others argue that privacy is personal and each individual should know how their personal data is being used. *Id.*

[10] *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9 ("Still, the majority of Americans are not confident about the way companies will behave when it comes to using and protecting their personal data.").

[11] *Id.*

[12] Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, THE N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

privacy policies and terms of service.[13] To illustrate this tension, as of May 2018, nearly three-quarters of Americans did not read terms of service or privacy policies carefully when signing up for social media networks.[14] In fact, 39% of millennials just clicked "agree" without even reading the terms or policy.[15] For millennials this was an increase of 5% from 2014.[16] While there is currently no data for 2020, the trend seems to be that fewer people—particularly—millennials, are reading terms of service when visiting social media websites.[17] Nonetheless, as of May 2018, 3 out of 5 Americans had little to no trust in social media companies with their information.[18] However, 40% of millennials had trust in social media sites despite failing to read website's fine print.[19] If fewer people are reading terms of service and online privacy policies, it is unlikely that more people will read lengthy privacy laws, much less take an active role in drafting effective legislation.

Politicians are now responding to these concerns. On February 12, 2020, Democratic Senator Kirsten Gillibrand of New York proposed that the United States create a Data Protection Agency to provide personal data protections in the digital age by way of sweeping federal regulations.[20] According to the Senator, it is now necessary for the United States to supply enhanced data protection to its citizens because the nation is "vastly behind other countries."[21]

This comment argues that a federal privacy regulation is necessary in order for the United States to keep up with the ever-changing privacy concerns of its citizens.[22] To address these concerns, Congress must first enact legislation that gives citizens privacy protections while crafting that legislation to survive challenges under the First Amendment and prohibit application of the Dormant Commerce Clause to state regulations. Ideally, this legislation would preempt and prohibit state-by-state applications of data regulations, as each state regulation includes differing protections of online privacy and access to personal information. This comment argues that current proposed solutions fail to account for the very fact that there is no fundamental right to privacy in the United States. Ultimately, in order for federal privacy legislation to survive the above-mentioned legal challenges, a fundamental right to privacy must be established in the United States. To illustrate the difficulty of such legislation, this comment addresses two differing protections of online privacy, most clearly illustrated by The General Data Protection Regulation[23]

---

[13] See *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9 for more statistics and research specifically about privacy policies and the way individuals interact with those privacy policies.

[14] Lincoln Park Strategies & Rad Campaign, *Fake News and Privacy: A Concern for Americans More Than Ever*, THE STATE OF SOC. MEDIA AND ONLINE PRIV. (May 2018), onlineprivacydata.com. Nearly one-quarter of Americans are asked to agree to privacy policies every day. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9.

[15] Lincoln Park Strategies & Rad Campaign, *supra* note 15. Interestingly, only 22% of adults in the United States "ever read privacy policies before agreeing to their terms and conditions . . . ." *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9.

[16] Lincoln Park Strategies & Rad Campaign, *supra* note 15.

[17] *See id.*

[18] *Id.* Only 63% of all Americans understand data privacy regulations. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9.

[19] Lincoln Park Strategies & Rad Campaign, *supra* note 15.

[20] Sen. Kristin Gillibrand (@gillibrandny), *The U.S. Needs A Data Protection Agency*, MEDIUM (Feb. 12, 2020), http://medium.com/@gillibrandy/the-u-s-needs-a-data-protection-agency-98a054f7b6bf.

[21] *Id.*

[22] Many scholars have proposed the idea of federal privacy regulation in the United States, and it has been a topic of discussion as the internet has dominated society.

[23] Regulation 2016/679 (General Data Protection Regulation), art. 94, 2016 O.J. (L 119) 1.

and the California Consumer Privacy Act, soon to be amended by the California Privacy Rights Act.[24]

First, this comment dives into the history and current privacy laws in the European Union to illustrate how the fundamental right to privacy in the European Union makes the GDPR successful. Section II focuses on the current patchwork of privacy laws of the United States, using California as an example of what a federal fundamental right to privacy may look like. Section III will briefly address the California Consumer Privacy Act, as amended by the California Privacy Rights Act, to assess its viability under both the Dormant Commerce Clause. That challenge will be critiqued and discussed in relation to the recent passage of the CPRA.

II. PRIVACY LAW IN THE EUROPEAN UNION

A. The History of Privacy Law in the European Union

In order to appreciate and understand the evolution of the General Data Protection Regulation ("GDPR") in the European Union, it must be understood that privacy in the European Union is a fundamental right, meaning that the right of privacy is explicitly protected in Title II, Article 8 of the European Charter of Fundamental Rights.[25] The recognition of this right allows the European Union to enact further laws and regulations that reflect the sweeping protection of this right to privacy.[26] More specifically, this right to privacy reflects the right to "protection of personal information," not merely privacy as it relates to niche areas such as children, criminal justice proceedings, or credit information, for example.[27] For now, this section will focus on Directive 96/45, which the GDPR replaced in 2018.

Directive 96/45[28] was adopted in the European Union on October 24, 1995 and addressed the protection of personal and individualized information.[29] The Directive established that the specific right to privacy must be balanced against competing interests such as artistic expression and journalistic purposes of media, to name a few.[30] With respect to journalistic purposes, the European Union has limited the right to privacy with respect to the literary and societal value of a journalistic publication in question.[31] The European Union Court of Justice has held that published media does not lose its journalistic purpose when the media contains personal information, for

---

[24] California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.105 (2018).
[25] Charter of Fundamental Rights of the European Union, 2012 O.J. (C.326) 391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[26] *See id; Data Protection*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection_en.
[27] Charter of Fundamental Rights of the European Union, 2012 O.J. (C.326) 391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[28] Formally titled the "protection of individuals with regard to the processing of personal data and on the free movement of such data." Directive 95/46, 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, 31.
[29] *Id.*
[30] *Id. See also* Charter of Fundamental Rights of the European Union, 2012 O.J. (C.326) 391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT; Joseph Savirimuthu, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC, to the Internet*, 25 J. MARSHALL J. COMPUT. & INFO. L. 241, 264 (2008).
[31] Högsta Domstolen [HD] [Supreme Court] 2001-6-12 Ö B 293-00 (Swed.), https://people.dsv.su.se/~jpalme/society/Ramsbro-HD-domen.html.

example, insulting judgements about other people.[32] The Court balanced the value of individual privacy rights laid out in the Directive against the freedom of expression and determined that the journalistic purpose of media outlives character attacks contained within the news stories.[33] As the internet and its information becomes more accessible, balancing these fundamental rights continues to get increasingly difficult and uncertain.[34]

Indeed, the importance of Directive 96/45 was the underlying principle that "data-processing systems are designed to serve man; whereas they must . . . respect their fundamental rights and freedoms . . . and contribute to economic and social progress . . . ."[35] The current "Right to Be Forgotten," codified in the Article 17 of the GDPR,[36] derives from *Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEDP),* which was decided May 13, 2014 by the European Court of Justice.[37] In that case, a resident of Spain, Mr. Gonzalez, alleged that reference to his personal information on a website by Google through search results violated his fundamental right to privacy.[38] First, Mr. Gonzalez wanted the website itself to delete the pages on which his personal information was included because the dispute to which the personal information related to had been settled several years ago in connection with legal proceedings.[39] While the Court determined that the website itself was not liable under Directive 96/45 because the information was legally contained within the page, the Court did make clear that obligations under the Directive were owed to individuals directly by the operators of the search engines, rather than the operators of the newspapers or links listed in the search results.[40] Mr. Gonzalez's request for Google to remove mentions of his name from search results that could lead to discovery of this personal information was thus accepted by the Court. [41]

This is to be distinguished from the type of processing carried out by publishers of websites whose website data appears in the search result list.[42] The Court took a strong stance regarding European Union citizen's fundamental rights by stating that the operators of any search engine

---

[32] *Id.* at 11.

[33] Joseph Savirimuthu, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC, to the Internet*, 25 J. MARSHALL J. COMPUT. & INFO. L. 241, 264 (2008) (quoting *Ramsbro*, B293-00 at 11).

[34] *See generally id.* at 264-65 (arguing that "it may be difficult to balance the competing interests such as, rights of expression and rights of privacy in such cases."). Interestingly, this article was written in 2008 but these two competing interests bear on the GDPR and protection of online privacy.

[35] Directive 95/46, 1995 O.J. (L 281) 31, 31 (EC).

[36] Regulation 2016/679 (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1. See below for a more in-depth discussion.

[37] Case C-131/12, Google Spain, SL v. Agencia Española de Prot. de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014).

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.* ("the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person . . . .").

[42] "It is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the later accessible to any internet user making a search on the basis of the data subjects name, including to internet users who otherwise would not have found the web page on which those data were published." Case C-131/12, Google Spain, SL v. Agencia Española de Prot. de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014). "Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users." *Id.*

must ensure the fundamental rights to privacy and the protection of personal data.[43] The Court further recognized that information from websites can be copied onto other websites, some of which are not subject to European Union legislation.[44] Therefore, the Court concluded that search engines are not able to wait until the personal information of data subjects has been erased on websites before de-listing the search engine results.[45] In effect, the search engine must simply de-list all relevant personal information without regard to whether that personal information has first been taken down by the individual websites, or if those websites were subject to European Union legislation to begin with.[46] Thus, with respect to the fundamental right to privacy, search engines are responsible under the Directive as data-processing systems, rather than individual websites.[47]

The acknowledgment by the Court that search engines themselves are subject to the Directive and now, the GDPR, makes those corporations responsible for the protection of individual personal data and individual privacy considerations.[48] This puts a large responsibility on the search engines. In effect, some may find it too difficult or cumbersome to follow European Union guidelines and thus find it not worth it to operate within the European Union.[49] This collateral effect is one of the many shortcomings of putting the protection and definition of personal data and privacy in the hands of corporations rather than the individual.

B. The Current Privacy Law in the European Union

Responding to a need to "provide legal certainty and transparency,"[50] the General Data Protection Regulation[51] took effect on May 25, 2018 and repealed Directive 95/46. This regulation, nearly identical to Directive 95/46 but with added protections, recognizes that an individual's fundamental right to privacy may be outweighed by the right to freedom of information and expression across the internet or other mediums.[52] There are six principles[53] that govern the GDPR. These principles are to be upheld by all businesses and organizations that qualify under the regulation and are as follows: (1) "lawfulness, fairness, and transparency"[54]; (2) "purpose

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] See section I.
[49] *The EU General Data Protection Regulation: Questions and Answers*, HUMAN RIGHTS WATCH (June 6, 2018 5:00am EDT), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation ("Although the GDPR is an EU regulation, it will affect the data practices of many organizations outside the EU.").
[50] Case C-131/12, Google Spain, SL v. Agencia Española de Prot. de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014).
[51] Regulation 2016/679, General Data Protection Regulation, of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46, 2016 O.J. (L 119) 1 (EU).
[52] *See id.*
[53] *Id.* at art. 5.
[54] *Id.* at 1(a).

limitation"[55]; (3) "data minimization"[56]; (4) "accuracy"[57]; (5) "storage limitation"[58]; and (6) "integrity and confidentiality."[59]

As a general provision, the European Union Court holds that it is not for individual newspapers, magazines, or online sources to take down information on individual webpages.[60] But it is for the *search engine* to take sufficiently effective measures, as codified in the GDPR and reinforced by Court decisions, to protect individual data subject's fundamental rights.[61] Search engines must also "seriously discourage[e]" all those internet users from accessing information related to an individual.[62] What is meant by "seriously discourage" is ill-defined and unclear, therefore, the extent of search engine obligations under the GDPR is up to differing interpretations.

As recently as 2018, the European Court of Human Rights held that a hyperlink posted on a website that led to a separate defamatory website fell within an exception[63] to an application of a strict liability standard for defamation.[64] The Court recognized that the primary purpose of hyperlinks is to call readers' attention to other material listed on a different website, and therefore acts as a connection to other sources of information.[65] Thus, the flow of information on the internet from hyperlinking material to which the original publication does not exercise control might have a "chilling effect," either directly or indirectly, on the freedom of expression on the Internet.[66]

The European Court of Justice's decision in *Google LLC v. Commission nationale de l'informatique et des libertes (CNIL)* determined that a search engine is not required to remove a link from all domain names used by the search engine in order to comply with the GDPR.[67] The practical effect of this requirement would be that if the operator did remove the links from all domain names, no links would appear within a search regardless of where the search took place and whether this search was from within the European Union or outside of it, such as in the United States.[68] Therefore, in order to address and combat some of the privacy interests at stake, Google proposed a "geo-blocking" feature.[69] This would block users in certain locations from accessing information, regardless of which version of Google the user was searching.[70] The individual's

---

[55] *Id.* at 1(b).
[56] *Id.* at 1(c).
[57] Regulation 2016/679, General Data Protection Regulation, of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46, 2016 O.J. (L 119) 1 (EU) at art. 5(1)(d).
[58] *Id.* at 1(e).
[59] *Id.* at 1(f).
[60] Case C-507/17, Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 ECLI:EU:2019:771, (Sept. 24, 2019).
[61] *Id.*
[62] *Id.*
[63] Regulation 2016/679, *supra* note 24 at art. 10. (Processing of personal data relating to criminal convictions and offences).
[64] Magyar Jeti Zrt v. Hungary, 2018 Eur. Ct. H.R. 1.
[65] *Id.*
[66] *Id.*
[67] Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019).
[68] *Id*; *see also* Ibrahim Hasan, *Google v CNIL and the Right to be Forgotten*, PUBLICLAWTODAY (Nov. 8, 2019), https://www.publiclawtoday.co.uk/information-law/344-information-law-features/41816-;
[69] Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019).
[70] *Id.*

location would be generated from an IP (Internet Protocol) address[71] so that Google could determine whether the individual was located within the European Union.[72] The Court balanced the fundamental right to privacy with the right to information and determined that this feature was an adequate solution by Google.[73]

While the Court recognized that the right to protect personal data is not an *absolute* right for citizens, a balancing test is used to determine how that right squares with the function of society and against other fundamental right—most importantly the freedom of expression and information.[74] Balancing these fundamental rights along with the necessary interests of the data controller differ with respect to the context in which the processing takes place. Thus, each balancing test determination varies significantly from case to case. [75] The Court stressed the fact that Member States must reconcile the differing protections of online privacy and how those states balance the fundamental right to privacy with the right of expression.[76] In fact, European Union law does not currently provide for cooperation between Member States, and those states have not come to a joint decision on how to apply this balancing test in relation to the scope of de-referencing information outside the physical boundaries of the European Union.[77] However, the Court concluded that this is for search engines themselves to figure out.[78]

The Court also recognized that balancing the right to privacy of internet users and access to information is likely to vary around the world.[79] The Court concluded that, based on the judgement in *Google Spain*, the subject of the search may request information to no longer be accessible to the general public through search results.[80] These individual "rights override . . . not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name."[81]

Although the European Union recognizes a fundamental right to privacy, Member States may balance the right to privacy with other rights, such as the right to free expression on the internet, differently than other States.[82] This patchwork of laws is representative of the way that

---

[71] "Each device that connects to the Internet needs a unique identifying number with which to communicate, called an 'IP address'". *What is an IP address?*, APNIC, https://www.apnic.net/get-ip/faqs/what-is-an-ip-address/ (last visited Jan 31, 2020).
[72] Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019).
[73] *Id.*
[74] EU Charter of Fundamental Rights, Title II, art. 11 ("Freedom of expression and information").
[75] *Id.* at 5.
[76] Case C-507/17, Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019); *Google LLC v. National Commission on Informatics and Liberty (CNIL)*, GLOBAL FREEDOM OF EXPRESSION, https://globalfreedomofexpression.columbia.edu/cases/google-llc-v-national-commission-on-informatics-and-liberty-cnil/ (last visited Jan 31, 2021).
[77] Case C-507/17, Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019) (stating that "[t]here is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction . . . to carry out such a de-referencing on all the versions of its search engine").
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*

the California Consumer Privacy Act fits in with the rest of the laws and regulations in the United States.[83]

III. PRIVACY LAW IN CALIFORNIA

California has led the way for social and political change around the country. It doesn't come as a surprise then that California's constitution formally recognizes both happiness and privacy as "inalienable rights" for citizens.[84] The state's unique recognition of the right to privacy slowly but surely paved the way for the California Consumer Privacy Act of 2018.

As early as 1931, the California Court of Appeals held that California citizens have a right to privacy.[85] The Court stated that the law of privacy was recent and cited *The Right to Privacy* by the Honorable Louis D. Brandeis and Samuel D. Warren in 1890.[86] That article influenced the national recognition of the right to privacy, although many states refused to formally recognize privacy as a fundamental right.[87] The Court recognized that private events may become public as a matter of public record, but nonetheless, the Court recognized that in California, the fundamental law of the state permitted the recognition of the "right to pursue and obtain safety and happiness without improper infringements thereon by others." [88]

The California courts expanded on this notion of private versus public information, eventually commenting on the nature of electronic communications. In 1971, the California Supreme Court criticized the role of media and electronic devices, "destroy[ing] an individual's autonomy, intrud[ing] upon his most intimate activities, and expos[ing] his personal characteristics

---

[83] *See, e.g., Practical Law Data Privacy Advisor, Demonstrating Compliance with the GDPR (2019).* The European Courts are not the only courts around the world to recognize the inherent difficulty when trying to apply different values of privacy and balance those values with other fundamental rights. For example, The Delhi High Court in 2019 issued an injunction against Google, Facebook, YouTube, and Twitter and directed those platforms to remove URLs that linked to defamatory information. *Ramdev v. Facebook*, GLOBAL FREEDOM OF EXPRESSION, https://globalfreedomofexpression.columbia.edu/cases/ramdev-v-facebook/ (last visited May 23, 2020). The Court viewed geo-blocking as an insufficient way to prevent access to the defamatory information while recognizing that this would necessarily call for a "global takedown order" and would threaten the free flow of information on the internet. *Id. See, e.g.,* Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, REGULATORY TRANSPARENCY PROJECT OF THE FEDERALIST SOCIETY (Dec. 2, 2019), https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf.

[84] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

[85] Melvin v. Reid, 297 P. 91, 91 (Cal. Ct. App. 1931). In this case, Gabrielle Darley a prostitute and was tried for murder which she was ultimately acquitted of. *Id.* After this, Darley "abandoned her life of shame and became entirely rehabilitated . . . [the next year she] commenced the duties of caring for their home, and thereafter at all times lived an exemplary, virtuous, honorable, and righteous life." *Id.* Darley mentioned to the Court that her friends did not know about her past. *Id.* However, in July 1925, a movie was released entitled "The Red Kimono," which was based upon Darley's past life, a true story. *Id.*

[86] *Id.* at 91. The Court distinguished California from other jurisdictions, "[t]he question is a new one in California. The only case to which we have been cited which even remotely relates to it is that of Crane v. Heine, 35 Cal. App. 466, 170 P. 433. This case, however, furnishes us with no authority for adopting in this state the doctrine of the right of privacy as it is known in other jurisdictions." *Id.* at 92; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (December 1890).

[87] *Melvin*, 297 P. at 92.

[88] *Id.* at 93.

to public gaze."[89] When determining whether an embarrassing yet truthful news article infringed on an individual's right to privacy, the Court considered the social value of the article and the offensive nature of the information contained in the article.[90] The Court noted that current events naturally spark media attention, and because that information has a high social value, constitutional protections are higher for newsworthy events.[91] Distinguishing those newsworthy events from the article at issue, the Court determined that this article did not serve an "independent public purpose," and thus the individual's privacy concerns outweighed First Amendment protections.[92]

That case was subsequently overruled by *Gates v. Discovery Comm., Inc* in 2004.[93] The Court took a step back from an individual's right to privacy, at least so far as it relates to facts available in public record.[94] The California Court concluded that prior Supreme Court decisions, specifically *Cox. v. Cohn*, undermined the recognition of an individual's fundamental right to privacy and favored broad First Amendment protections for news articles.[95] Importantly, the Court recognized that under federal constitutional law principles and common law, the right to privacy is difficult to recognize as a fundamental right.[96] Thus, while happiness and privacy are both "inalienable rights" under the California constitution, courts have had difficulty balancing these rights with other constitutional protections such as the First Amendment.[97]

IV. THE CCPA

A. What is the CCPA?

The California Consumer Privacy Act ("CCPA") includes many different provisions, but this section will focus specifically on § 1798.105 of the California Civil Code as amended by the Act[98]. The goals of the CCPA expand on the existing right to privacy in the United States and provide Californians with data privacy protections in order to control the use of personal information.[99] The California legislation was approved a month after the GDPR went into effect, and is the strictest personal data privacy regime in the United States.[100] The Act only applies in California and to California residents, however making compliance by internet companies that engage in business within the United States inherently difficult.[101]

---

[89] Briscoe v. Reader's Digest Ass'n.,483 P.2d 34, 37 (1971).
[90] *Id.* at 38.
[91] *Id.* at 40.
[92] *Id.* at 39-40 (relying on A. Meiklejohn, *Political Freedom: The Constitutional Powers of the People* (1960)).
[93] *See* Gates v. Discovery Comm., Inc., 101 P.3d 552 (Cal. 2004).
[94] *Id.* at 562.
[95] *Id. See* Victor P. Muskin, *The Right to Be Forgotten: Are Europe and America on a Collision Course?*, 91 N.Y. ST. B.J. 36 (March, 2019).
[96] *Gates*, 101 P.3d at 573. *See also S*haun G. Jamison, *Creating a National Data Privacy Law For the United States*, 10 CYBARIS AN INTELL. PROP. L. REV. 1, 7 (2019) for a discussion on a federal right to privacy.
[97] *See* Gates v. Discovery Comm., Inc., 101 P.3d 552 (Cal. 2004).
[98] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.105 (2018).
[99] *About the California Consumer Privacy Act*, CALIFORNIANS FOR CONSUMER PRIVACY, https://www.caprivacy.org/about (last visited Jan. 17, 2020).
[100] Szuyin Leow, *The California Consumer Privacy Act Arrives in January 2020. What Can We Expect?*, LOGICATE (Feb. 12, 2019), https://www.logicgate.com/2019/02/12/the-california-consumer-privacy-act-arrives-in-january-2020-what-can-we-expect/.
[101] *Id.*

The CCPA requires a business to comply with customer requests to delete personal information[102] if the customer requests that deletion, unless it is necessary for the business to collect this personal data.[103] The Act gives Californians specific privacy rights, including: (1) the right to know what personal information is collected about the consumer; (2) the right to know whether that information is sold or disclosed, and to whom; (3) the right to say no to that sale; (4) the right to access that information; and (5) the right to equal treatment by the business.[104]

California is just one of eleven states that recognize privacy as an enumerated right in its state constitution.[105] However, balancing one state's fundamental right of privacy with federal constitutional law principles is difficult at best.[106] In order to determine whether the CCPA comes into conflict with federal constitutional principles, it is necessary to analyze the Act under the Dormant Commerce Clause.

B. Dormant Commerce Clause Challenge

A central constitutional challenge to the CCPA is the Dormant Commerce Clause, which prohibits discrimination between in state and out-of-state citizens.[107] When Congress or the Supreme Court has not preempted an area of state legislation, state legislation is analyzed under strict or intermediate scrutiny in order to be constitutional.[108] The following analysis focuses on the challenges of the CCPA under this Constitutional principle.[109]

Article I of the United States Constitution supports the principle that state and local laws may not burden commerce between the states more than necessary.[110] When challenging a state regulation under the Dormant Commerce Clause, the first question for the court is whether the state legislation is an "illegitimate means of isolating a state from the national economy," and thus is facially discriminatory (a per se violation of the Dormant Commerce Clause).[111] Discrimination means "differential treatment of in-state and out-of-state economic interests that benefits the

---

[102] The Act defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." West's Ann. Cal. Civ. Code § 1798.140. This includes, but is not limited to, "inferences drawn . . . to create a profile about a consumer reflecting . . . preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." *Id.* While the CCPA does not include publicly available information "lawfully made available from federal, state, or local government records," the definition of "personal information" is vague, broad, and unspecific. CCPA, Section 1798.140(o)(2); *see* David Zetoony, *CCPA Privacy FAQs: Does "personal information" include information that a business obtains from government records?*, JDSUPRA (July 17, 2019), https://www.jdsupra.com/legalnews/ccpa-privacy-faqs-does-personal-17583/ (last visited Feb. 23, 2020) ("The CCPS was put together quickly (in approximately one week). Given its hasty drafting, there are a number of instances in which the act is at best ambiguous and at worst unintelligible.").

[103] CALIFORNIA LEGISLATION INFORMATION, AB-1760 CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (2019); Alan S. Gutterman, *California Consumer Privacy Act of 2018*, Bus. Transactions Solutions § 230:38.50.

[104] *Id.*

[105] *Id.; Privacy Protections in State Constitutions*, NCLS, https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (last visited May 27, 2020).

[106] *See, e.g.*, Huddleston & Adams, *supra* note 84.

[107] *See, e.g*, Pike v. Bruce Church, Inc., 397 U.S. 137 (1970).

[108] *See id.*

[109] For an in-depth discussion, *see* Russell Spivak, *Too Big a Fish in the Digital Pond? The California Consumer Privacy Act and the Dormant Commerce Clause*, 88 U. CIN. L. REV. 475 (2019); Huddleston & Adams, *supra* note 84.

[110] Huddleston & Adams, *supra* note 84.

[111] City of Philadelphia v. New Jersey, 437 U.S. 617, 627 (1978).

former and burdens the latter."[112] These laws are subject to the strictest scrutiny, as economic protectionism is not a legitimate means to "evenhandedly [] effectuate a legitimate local public interest."[113] When state legislation is an "illegitimate means of isolating the state from the national economy," this state law will be facially discriminatory towards out-of-state commerce.[114] When a law is not facially discriminatory, the law is subject to the *Pike* balancing test.[115] This test is conducted by answering the following four questions of the state regulation: (1) whether the regulation is even-handed; (2) whether the regulation effectuates a legitimate purpose; (3) whether the regulation's effects on interstate commerce are incidental; and (4) whether the burden of the state regulation is excessive in relation to local putative benefits.[116]

The argument that the CCPA does not violate the Dormant Commerce Clause relies in part on *Healy v. Beer Institute, Inc.*, in which the Supreme Court of the United States determined that when a state regulates commerce occurring "wholly outside" that State's borders, that regulation is invalid.[117] Scholars argue that the language of the CCPA, specifically the language in § 1798.140(c)(1) that only those businesses that actually "do[] business in the State of California" precludes application of the extraterritoriality test to the CPPA, while others write this extraterritorial test off as inapplicable except to those cases of price-fixing, such as in *Healy*.[118]

However, the 2nd Circuit Court of Appeals in *American Bookstores* recognized that because there are no recognized geographical boundaries within the internet, it is nearly impossible for a state to regulate those activities on the internet without "project[ing] its legislation into other states."[119] In that case, the Court struck down a law prohibiting dissemination of sexually harmful materials to children over the internet.[120] The Court determined that Vermont's interest was "impracticable" because the Vermont law prohibited Vermont, but not other states, from viewing certain materials.[121] Importantly, the Court noted that the internet may soon be protected from state-by-state regulations.[122] Thus, the burdens imposed by the CCPA do not end with the corporation who is directly affected but will instead create a domino effect of far-reaching implications for those business who regularly use personal data.[123]

---

[112] Spivak, *supra* note 110, at 495 (quoting Oregon Waste Sys., Inc. v. Department of Envtl. Quality, 511 U.S. 93, 99 (1994)).
[113] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).
[114] *Philadelphia v. New Jersey*, 437 U.S at 627.
[115] Nicholas F. Palmeri, *Who Should Regulate Data?: An Analysis of The California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws*, 11 Hastings Sci. & Tech.L.J. 37, (2020).
[116] *Pike*, 397 U.S. at 142. For a more in-depth discussion, *see* Palmeri, *supra* note 116.
[117] Healy v. Beer Institute, Inc., 491 U.S. 324, 332 (1989).
[118] Spivak, *supra* note 110. While this article does not go into great detail about the different tests under the Dormant Commerce Clause analysis, the extraterritorial argument is the primary analysis used to determine whether the CCPA is invalid. *See, e.g.*, Kiran K. Jeevanjee, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U. L. REV. F. 75, 75 (2020); Mallory Ursul, *The States' Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause*, 52 SUFFOLK U.L. REV. 577, 578 (2019); Palmeri, *supra* note 116.
[119] *American Booksellers Foundation v. Dean*, 342 F.3d 96, 103 (2d Cir. 2003) (quoting *Healy*, 491 U.S. 324 at 334).
[120] *Id.* at 102.
[121] *Id.* at 103-04 ("A person outside Vermont who posts information on a website or on an electronic discussion group cannot prevent in Vermont from accessing the material. If someone in Connecticut posts material for the intended benefit of other people in Connecticut, that person must assume that someone from Vermont may also view the material. This means those outside Vermont must comply with [the law]. . . .").
[122] *Id.* at 104.
[123] Huddleston & Adams, *supra* note 84, at 8.

The scholars who only look to the language of the CCPA or who write off the extraterritorial analysis as inapplicable are mistaken to do so. Admittedly, it is difficult to argue that the CCPA regulates something that is occurring "wholly outside" the state's borders; however, the internet, social media, and online data regulations do not follow along the border of *any* state.[124] While the CCPA may *say* that the regulation only applies to those businesses doing business in California, the stringent requirements for compliance under the regulation impact other businesses not yet doing business in California. For example, some of those businesses may have chosen not to do business in California and may never do so because it is too difficult or expensive to comply with the requirements under the CCPA. The corporations located within California are now faced with a new reality: either comply with the most comprehensive privacy Act in the country or stop doing business in California.[125]

The CPRA may nonetheless save the CCPA from an extraterritorial argument.[126] As currently written, the CPRA has increased the number of California residents of which businesses "buy, sell, or share" the personal information of from 50,000 to 100,000.[127] This increase raises the threshold that a business must reach in order to be regulated by the CCPA, in turn creating more of a limitation on the businesses that are considered to do business in California.

An additional consideration under the Dormant Commerce Clause is whether states such as Maine[128] and Nevada[129] expand current privacy regulations to be as comprehensive as the CCPA.[130] A federal fundamental right to privacy, and as a result, federal privacy regulation, would preempt these state laws and effectively prohibit any application of the Dormant Commerce Clause to these swiss-cheese like state regulations.[131]

V. CONCLUSION

The internet will continue to impact society in the future, which renders it necessary to determine how differing privacy laws will affect how global citizens interact with one another,

---

[124] See Section I(A).
[125] Huddleston & Adams, *supra* note 84, at 8-9.
[126] For more information on what is included in the CPRA, see *CCPA vs. CPRA - What Has Changed?*, ONETRUST (Nov. 10, 2020), https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/.
[127] *Id*.
[128] The Maine Privacy Law, LD 946, only applies to internet service providers, and thus is not nearly as comprehensive as the CCPA. An Act To Protect The Privacy of Online Customer Information, 1 M.R.S. § 9301 (2019); *see also* Lothar Determann & Helena J. Engfeldt, *Maine and Nevada's New Data Privacy Laws and the California Consumer Privacy Act Compared*, BAKERMCKENZIE (June 20, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/06/maine-and-nevada-new-data-privacy-laws.
[129] Nevada Senate Bill 220 limits the type of information protected. *See* Nev. Rev. Stat § 603A (2019); *see also* Lothar Determann & Helena J. Engfeldt, *Maine and Nevada's New Data Privacy Laws and the California Consumer Privacy Act Compared*, BAKERMCKENZIE (June 20, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/06/maine-and-nevada-new-data-privacy-laws.
[130] "[I]f multiple states adopted comprehensive date privacy legislation . . . conflicting state privacy regulations resulting in unreasonable or even impossible compliance could support . . . extraterritoriality." Mallory Ursul, *The States' Role in Data Privacy: California Consumer Privacy Act Versus Dormant Commerce Clause,* 52 SUFFOLK U. L. REV. 577, 601 (2019).
[131] For more information on one federal privacy approach, see Cameron F. Kerry & John B. Morris, Jr., *Preemption: A balanced national approach to protecting all Americans' privacy*, BROOKINGS (June 29, 2020), https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy/.

whether that is across the room or across the world.[132] By analyzing privacy with this perspective in mind, a better understanding of what privacy means in a digitized world will guide future discussions to allow for beneficial privacy legislation.[133] As discussed above, although social media has increased at alarming rates just within the past few years, the internet has not reached its peak.[134] Privacy laws, both past and current, have worked for a short moment. As technology continues to grow, it is more important than ever to assign privacy value in relation to other constitutional protections and to define what privacy means in the digital age.[135]

In the European Union, Directive 96/45 set the foundation for the "Right to be Forgotten."[136] Member States have acknowledged the difficulty of balancing individuals' expression interests with the fundamental right to privacy.[137] Courts have determined that it is the responsibility of the search engine to adequately protect personal data, which in effect puts the privacy conversation in the hands of corporations.[138] Similarly, in the state of California, United States, the fundamental law of the state has permitted the courts to formally recognize a fundamental right to happiness and privacy, although squaring this right with other constitutional protections, such as the First Amendment, has proven challenging.[139]

The California Consumer Privacy Act of 2018 is the most sweeping data protection regime currently in effect within the United States.[140] However, this Act has several significant hurdles to jump over before consumers should blindly accept the consequences that will soon affect the accessibility of information worldwide and between the states.[141] The Act will be modified by the CPRA in 2023, however, which may save the CCPA for failing under the Dormant Commerce Clause.[142]

Federal legislation in the United States fails to account for internet privacy in a comparable way to both the CCPA and the GDPR.[143] The United States Congress should draft federal legislation that will ultimately preempt state laws such as the CCPA and prevent those laws to be applied on a state-by-state basis.[144] First, however, privacy must be established as a fundamental right, specifically enumerated in the Constitution of the United States.

There are no geographical boundaries on an Instagram or Facebook page. It is possible to message a person on the opposite side of the world. A picture on Instagram may go "viral" in a number of minutes. Technology and the internet are here to stay. Social media, news outlets, and the access to unlimited information at individual fingertips comes with a price, and it is likely that

---

[132] *See, e.g., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9; Kat Smith, *supra* note 2; Palmeri, *supra* note 116; Spivak, *supra* note 110.
[133] *See, e.g., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, *supra* note 9; Kat Smith, *supra* note 2; Palmeri, *supra* note 116; Spivak, *supra* note 110.
[134] *See* Kat Smith, *supra* note 2.
[135] *See, e.g.,* Spivak, *supra* note 110; *What is Global Citizenship?*, *supra* note 6.
[136] Regulation 2016/679 (General Data Protection Regulation), art. 94, 2016 O.J. (L 119) 1.
[137] See Case C-131/12, Google Spain, SL v. Agencia Española de Prot. de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014) and Magyar Jeti Zrt v. Hungary, 2018 Eur. Ct. H.R. 1 for illustration of this principle.
[138] Case C-507/17, Google LLC v. Commission nationale de I'informatique et des libertes (CNIL), 2019 EUR-Lex CELEX LEXIS 772 (Sept. 24, 2019). See Section I for discussion of the corporation-controlled privacy conversation.
[139] *See* Gates v. Discovery Comm., Inc., 101 P.3d 552 (Cal. 2004).
[140] Tami Abdollah, *California Passes Nation's Most Stringent Consumer Data Privacy Law*, DOT.LA (Nov. 4, 2020), https://dot.la/california-proposition-24-2648623072/twitter.
[141] Huddleston & Adams, *supra* note 84.
[142] *CCPA vs. CPRA - What Has Changed?*, *supra* note 127.
[143] *See* Muskin, *supra* note 96.
[144] *Preemption: A balanced national approach to protecting all Americans' privacy*, *supra* note 132.

"price" is the inherent loss of individual privacy if that determination is left up to the corporation and privacy is not regarded as a fundamental right within the United States.