Do We Own What We Post?: The Fundamental Property Right to Destroy Your Presence on the Internet

*Olivia Shangrow**

CONTENTS

"Every [one] has a property in [their] own person. This nobody has a right to, but [themself]."

-John Locke[1]

* J.D. Candidate 2023, Seattle University School of Law. Thank you to the entire Law Review team and to Professor Steve Tapia for the assistance in the development of this Note. I am additionally grateful to my husband, Graham Bradley, for all his support.

1. JOHN LOCKE, SECOND TREATISE § 27 (1689).

INTRODUCTION

Someone can buy your social security number for $0.53.[2] The going rate for your banking records is $4.12.[3] Our personal data is the most sought-after asset for companies vying for the most effective way to advertise to us online. Facebook could fill 367,873 pieces of paper with the personal information it has collected about you,[4] and it relies on such information to make money.[5] In 2018, in the United States alone, Facebook sold your name, likes, dislikes, shopping habits, political preferences, location, and more to other companies at a valuation of 11.9 billion dollars.[6] In 2022, said data is now worth $40.5 billion.[7] And Facebook is just one player in the vast data market. The projected value in 2022 of our personal information sold by different companies on the Internet[8] is $197.65 billion, more than the total value of U.S. agricultural output.[9] Motivated by the extreme amount of revenue our personal information now generates each year, very personal aspects of our lives have been commodified in shocking ways:

- Data brokers, whose sole purpose is to compile and sell your information to other companies, have offered for sale horrifying lists containing names of people thought to be experiencing erectile dysfunction or alcoholism and survivors of sexual assault.[10]

---

2. *How Much Is Your Data Worth? The Complete Breakdown for 2021*, INVISIBLY (July 13, 2021), https://www.invisibly.com/learn-blog/how-much-is-data-worth [https://perma.cc/EJ5Y-BWMW].

3. *Id.*

4. ROBERT SHAPIRO & SIDDHARTHA ANEJA, FUTURE MAJORITY, WHO OWNS AMERICANS' PERSONAL INFORMATION AND WHAT IS IT WORTH? 1 (2019), https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf [http://perma.cc/W4QM-F28H].

5. *Id.* at 7. Personal information collected and sold by Facebook makes up 98% of Facebook's yearly revenue. *Id.*

6. *Id.* at 3.

7. *Id.* at 4.

8. Controversial to some, this Note maintains the usage of a capital I in the spelling of Internet throughout. Modern trends indicate that the word is so widely used, that its capitalization as a proper noun is no longer necessary. *See* Susan C. Herring, *Should You Be Capitalizing the Word 'Internet'?*, WIRED (Oct. 19, 2015), https://www.wired.com/2015/10/should-you-be-capitalizing-the-word-internet/ [http://perma.cc/AT2K-6YGN]. However, I maintain the capitalization in recognition that the Internet, in its current globalized form, is a "unique entity," and thus should be capitalized to set it apart from other smaller computer networks. *Id.* More broadly, as this Note speaks to the way the Internet has shaped how our data is shared and sold, this stylistic choice acknowledges the practically immeasurable size of the Internet and its integration into our lives.

9. SHAPIRO & ANEJA, *supra* note 4, at 5.

10. Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'*, FORBES (Dec. 19, 2013), https://www.forbes.com/sites/kashmirhill/2013/

- Facebook has given the dating site OkCupid access to users' dating and sexual information.[11]
- PayPal shares users' personal data with over 600 companies worldwide.[12]
- Spotify, Netflix, and the Royal Bank of Canada were allowed access to private messages between Facebook users.[13]
- Anti-abortion groups purchase location data of people who recently visited a Planned Parenthood location.[14]
- Marco Rubio made $504,651 from selling his contributors' data after dropping out of the presidential race in 2016.[15]
- Donald Trump's team purchased location data of users known to attend certain types of churches.[16] The Trump campaign then offered donors' names, emails, and phone numbers for sale, charging $35 per 1,000 people.[17]
- Flo, a menstrual cycle tracking app, sold information about "users' periods, pregnancies, and childbirth."[18]
- An app that's sole purpose is to open and close your garage door collects and sells information about when and how often you leave the house.[19] The list goes on.

12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/?sh=46df4541d535 [https://perma.cc/74HL-P5F2]. A list of 1,000 names of people thought to fall into one of these categories costs $79. *Id.*

11. SHAPIRO & ANEJA, *supra* note 4, at 15.

12. *List of Third Parties (Other Than PayPal Customers) with Whom Personal Information May Be Shared*, PAYPAL, https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list [https://perma.cc/8D2E-7S2P]. A list of third parties is disclosed on PayPal's website, a practice required by European privacy laws, *see infra* Part II.

13. SHAPIRO & ANEJA, *supra* note 4, at 7.

14. Makena Kelly, *Steve Bannon Used Location Targeting to Reach Voters Who Had Been in Catholic Churches*, THE VERGE (July 19, 2019), https://www.theverge.com/2019/7/19/20700866/steve-bannon-location-data-carriers-tmobile-att-verizon [https://perma.cc/JB2N-A5N7].

15. Jose Pagliery, *Here's How Presidential Candidates Sell Your Personal Information*, CNNMONEY (July 7, 2016), https://money.cnn.com/2016/07/07/news/presidential-candidate-sell-donor-data/index.html [https://perma.cc/NGM8-8LZ3].

16. Kelly, *supra* note 14.

17. Maggie Haberman & Kenneth P. Vogel, *Trump Campaign Selling Email and Phone Lists for Millions of Supporters*, SEATTLE TIMES (Oct. 13, 2018), https://www.seattletimes.com/nation-world/trump-campaign-selling-email-and-phone-lists-for-millions-of-supporters/ [https://perma.cc/2NC5-LLQ2].

18. Natasha Singer, *Flo Settles F.T.C. Charges of Misleading Users on Privacy*, N.Y. TIMES (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/business/flo-privacy.html [https://perma.cc/QK2A-NK9G].

19. Shira Ovide, *Facebook Is Hated—And Rich*, N.Y. TIMES (Jan. 28, 2021), https://www.nytimes.com/2021/01/28/technology/facebook-earnings-reputation.html [https://perma.cc/6GYY-2RW].

There is a major conflict between businesses that collect and sell our data and what kind of data protections individuals are afforded when fundamental rights are extrapolated to the Internet. While the United States and Europe both recognize a fundamental right to privacy,[20] fundamental property rights recognized in the physical world are not currently being represented in our online personas. As a result, the right to control our data in their current form is functionally meaningless; we cannot interact with our online property in the same way we can our physical property: by excluding others, controlling how others use it, or the ultimate property right—the right to destroy. By shifting our focus of developing data privacy legislation through a purely personal privacy lens to include the framework already established by property law, we can create an online ecosystem allowing for the real expression of personal property rights, including the fundamental right to destroy one's own property.

This Note will explore the well-established right to destroy your own property and how such a fundamental right can and should be applied to our online property to develop more protective data privacy legislation. Part I highlights the longstanding pillar of property law establishing a right to destroy one's property, and how that can and should be applied to your digital identity. Part II will discuss the ambiguity of personal data ownership online and the ill effects resulting from the lack of control of our personal information on the Internet. Part III examines the current state of data privacy legislation in Europe and the first several states to enact their own data privacy laws. Finally, Part IV will comment on the shortcomings of Washington State's proposed data privacy legislation and how a recognition of online property rights would cement greater protections for individuals both on and off the Internet.

I. THE FUNDAMENTAL RIGHT TO DESTROY ONE'S OWN PROPERTY

The right to destroy is a fundamental property right recognized by almost all legal systems around the world.[21] This powerful right gives owners of property ultimate control over the destiny of their personal belongings. This property right creates a demarcation of the boundaries of what we can do with our own property; if we are given the right to destroy property, we necessarily have the right to "use or dispose of [the property]

20. *See, e.g.*, Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Griswold v. Connecticut, 381 U.S. 479 (1965); EUROPEAN CONVENTION ON HUMAN RIGHTS, COUNCIL OF EUROPE 11 (1950).

21. JOHN G. SPRANKLING, THE INTERNATIONAL LAW OF PROPERTY 293 (2012).

in a less dramatic manner."[22] While this right has been deemed inappropriate over time in some contexts relating to property with great cultural heritage or artistic value,[23] American courts have long upheld its place in property law.[24] This right is also mirrored in state legislation: to be found in violation of a criminal damage statute, the property must be identified as property "of another."[25] Property damage to one's own property is not a crime. In fact, the right to destroy is so fundamental it is included in first-year property law school curriculum as part of the "bundle of rights," alongside the right to use, consume, and transfer.[26] The right to destroy is the epitome of ultimate control over the relationship between an owner and a thing; destruction enables that relationship to be severed or made extinct.[27] The ability to permanently disassociate oneself from property has great personal security ramifications, particularly in a digital landscape where we upload and share our identity, personal finances, employment, and reputation.

With the integration of the Internet into our daily lives, the question arises of how this fundamental property right transfers to our digital property. To add complication to answering this question, we do not have a succinct definition of what comprises digital property.[28] As a general explanation, personal data has been:

> roughly defined as a living data subject's name combined with other nonpublic information. Protected data may relate to an individual's account, e-mail address, IP address, registration, health, economic

---

22. Lior Jacob Strahilevitz, *The Right to Destroy*, 114 YALE L. J. 781, 788 (2005). Jurist William Blackstone stated: "if a man be the absolute tenant in fee-simple . . . he may commit whatever waste his own indiscretion may prompt him to, without being impeachable or accountable for it to [anyone]." WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, at Book III, ch. 14 (1753).

23. *See, e.g.*, SPRANKLING, *supra* note 21, at 298–302; *see generally* JOSEPH SAX, PLAYING DARTS WITH A REMBRANDT (1999).

24. *See, e.g.*, Bloss v. Tobey, 19 Mass. 320, 341 (1824) (it is not unlawful to burn down your own store); U.S. v. Vanranst, 28 F. Cas. 360, 360 (C.C.D. Pa. 1812) (owner of boat could destroy the vessel without committing any crime); Cass v. Home Tobacco Warehouse Co., 223 S.W.2d 569, 571 (Ky. 1949) (dispute over damaged property, court held that "they had the right to destroy it if they were holding the property at that time under the terms incorporated in the written lease").

25. *See, e.g.*, WASH. REV. CODE § 9A.48.080(1) ("A person is guilty of malicious mischief in the second degree if he or she knowingly and maliciously: (a) Causes physical damage to the property of another"); *see also* ARIZ. REV. STAT. ANN. § 13-1602 ("A person commits criminal damage by: 1. Recklessly defacing or damaging property of another person.").

26. J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 741 (1996).

27. *Id.* at 759.

28. *See* Kevin Dong, *Developing a Digital Property Law Regime*, 105 CORNELL L. REV. 1745, 1747 (2020); *see also* Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 5 ("[T]here is much uncertainty and ambiguity regarding the meaning of 'data,' 'information,' and 'ownership;' little comprehensive analysis regarding how existing property laws already cover data or exclude data from protection; and relatively sparse considerations of legal and policy reasons for *not* granting property rights to data.").

> status, ethnicity, race, sexual preference, religion, political affiliation, union membership, criminal records, education, photos, and much more.[29]

Some kinds of virtual property, such as images and video files, are more analogous to tangible physical property and, therefore, more easily align with conventional definitions of property.[30] However, some suggest online accounts, such as social network accounts, are "assets in and of themselves and have value to an estate."[31] And while copyright law tells us that we cannot own facts,[32] the nature of our digitized lives has transformed our personal information into a commodity.[33] The recognition of personal information as a valuable asset has also raised unjust enrichment[34] concerns suggesting that "it may be unfair for such personal data handlers to capitalize on an asset that would not exist without the person who is the subject of the personal information."[35]

Although policy and legal decisions have not caught up yet, digital property should be viewed as comprised not only of digital objects, such as files that have been purchased, uploaded, or downloaded, but also of our personal data that is the currency of online monoliths like Facebook, Google, and YouTube. As Daniel Martin emphasizes in his article regarding online property, "increasing prevalence of cloud computing provides a new context for reexamining, and a new justification for reaffirming, the right to destroy."[36] The integration of our data in a myriad of online businesses, including the exploitation of our information by data brokers and social media platforms, reaffirms the need for the right to destroy to extend throughout our entire online persona.

---

29. ALEX SAMUEL, COMMON THEMES AMONG PERSONAL DATA PROTECTION LAWS, 2 DATA SEC. & PRIV. L. § 15:2 (2021–2022).

30. John Romano, *A Working Definition of Digital Assets*, THE DIGITAL BEYOND (Sept. 1, 2011), http://www.thedigitalbeyond.com/2011/09/a-working-definition-of-digital-assets/comment-page-1 [https://perma.cc/3LNJ-84X5].

31. *Id.*

32. *What Does Copyright Protect?,* U.S. COPYRIGHT OFFICE, https://www.copyright.gov/help/faq/faq-protect.html [https://perma.cc/55CV-SNBV]. "Copyright does not protect facts, ideas, systems, or methods of operation, although it may protect the way these things are expressed." *Id.*

33. JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY AND THE NEW DIGITAL SERFDOM 17 (2017).

34. Unjust enrichment is defined as "[a] benefit obtained from another, not intended as a gift and not legally justifiable, for which the beneficiary must make restitution or recompense." *Unjust Enrichment*, BLACK'S LAW DICTIONARY (11th ed. 2019).

35. Dorothy J. Glancy, Personal Information as Intellectual Property 3 (unpublished manuscript) (on file with author).

36. Daniel Martin, *Dispersing the Cloud: Reaffirming the Right to Destroy in a New Era of Digital Property*, 74 WASH. & LEE L. REV. 467, 473 (2017).

II: READING THE FINE PRINT OF DATA PRIVACY: WHAT DO WE OWN, AND DOES ANYTHING BELONG TO THE COMPANIES?

As the Internet has become central to our daily lives, we are buffered at every moment by "comprehensive digital memory."[37] Unlike the very human-centric behavior of forgetting, the Internet remembers all. It remembers every online search, every status update, and every transaction. Of this seemingly infinite amount of information about each of us that perpetuates online, what remains our own rather than a digital asset belonging to the platform that collects it?

Many companies' terms of service pages address this question in simple terms. For example, Twitter announces to users: "You retain your rights to any Content you submit, post or display on or through the Services. What's yours is yours—you own your Content (and your incorporated audio, photos[,] and videos are considered part of the Content)."[38] Likewise, Facebook users "own the intellectual property rights (things like copyright or trademarks) in any such content that you create and share on Facebook . . . . Nothing in these Terms takes away the rights you have to your own content."[39] These companies feign as though users' property rights have not been abdicated under these terms. By requiring users to agree to grant an unlimited use license, these companies create a façade downplaying the massive value they grant to themselves through this use license. For example, Facebook retains a "non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content."[40] Twitter maintains these same rights as well as the ability to "reproduce, process, adapt . . . publish, transmit . . . in any and all media or distribution methods now known or later developed."[41] But neither of these sets of terms define any entitlements, or even promises, about the data you create simply by being on the platform. With these licenses, Facebook has turned its "friendly neighborhood social network"[42] into a cash cow.[43]

---

37. VIKTOR MAYER-SCHONBERGER, THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 11 (2009).

38. *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos [https://perma.cc/7PNB-3VT5].

39. *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/R4H4-35A3].

40. *Id.*

41. *Twitter Terms of Service*, *supra* note 38.

42. Chaim Gartenberg, *What Is Facebook? Just Ask Mark Zuckerberg*, THE VERGE (Mar. 8, 2019), https://www.theverge.com/2019/3/8/18255269/facebook-mark-zuckerberg-definition-social-media-network-sharing-privacy [https://perma.cc/VN97-Q7E7].

43. See footnotes 4–7 and accompanying text for a discussion of the profits that Facebook has made from compiling and selling our personal information.

These seemingly all-encompassing licenses make online ownership of content, or control of personal data, functionally meaningless; users no longer have a bundle of rights regarding online property ownership. Users cannot exclude others from their online property, as these companies are allowed to sub-license the content to other entities. Users cannot control the usage of their online property; these companies can manipulate, alter, perform, or distribute the content as they wish. Users cannot control the enjoyment of their online content; companies can copy and share at their discretion. And ultimately, users have lost the ability to destroy their content. As Facebook plainly states in its terms of use,

> You can delete content . . . . When you delete content, it's no longer visible to other users, however it may continue to exist elsewhere on our systems where . . . your content has been used by others in accordance with this license and they have not deleted it . . . ."[44]

The only choices users are afforded are to comply with the loss of their fundamental property rights or discontinue use on these platforms.

Beyond the social networking companies, there is a vast network of data brokers, companies specializing in collecting personal information and selling that collection of data to other companies.[45] Acxiom, one of the largest of these companies, promises to "allow you to know your customer at a whole new level."[46] By using public records, credit card purchases, and social media posts, Acxiom has collected data on over 500 million consumers; by 2012 metrics, data broker companies made $150 billion in revenue from their services.[47] Acxiom acknowledges the potential threat data privacy legislation poses to its business model, stating on its website:

> The future demise of third-party cookies will have a negative impact on people's experience by reducing the effectiveness of a marketer's ability to personalize messaging and eliminate the ability to measure true attribution. The implications of cookie deprecation on digital personalization and ad tracking, as well as privacy will be far reaching.[48]

---

44. *Terms of Service*, *supra* note 39.

45. Dan Rafter, *How Data Brokers Find and Sell Your Personal Info*, NORTON, https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html [https://perma.cc/8UZU-XPNM].

46. *Data Enrichment*, ACXIOM, https://www.acxiom.com/customer-data/enrichment-data/ [https://perma.cc/A5RW-6XXE].

47. Rafter, *supra* note 45.

48. *Marketing Solutions*, ACXIOM, https://www.acxiom.com/media-marketing-solutions/ [https://perma.cc/3LFC-7NS2].

After years of companies massively profiting from our collective unawareness about their personal-data-for-profit business model, the acknowledgment that Internet users disfavor the idea of commodification of personal information is becoming more widely recognized. The 2020 Internet Advertising Revenue Report's "vision for the future" plainly states:

> Consumers no longer think the exchange of free content for ad delivery is good enough—the value exchange must be reset . . . . How consumers engage with brands and content—and think about who they trust with their data—has evolved. As a result, the presumed value exchange of ad-supported media—free content in exchange for seeing ads—is losing its persuasive power.[49]

Ironically, framing the collection and distribution of our personal information as an exchange between the user and the business creates the framework for acknowledging our personal data is a valuable entity deserving of property rights.

Why should we care companies are utilizing our personal data as currency? Internet users are familiar with the practice of acquiescing to terms of use in order to navigate, read, purchase, or otherwise use just about any website. However, "[c]onsent for limited use of data is not a license for its viral spread."[50] Consent is especially meaningful given the abundance of personal information online, which can "be a source of embarrassment, acrimony, surveillance, and stalking."[51] Indeed, there are many stories of colleges and employers using social media postings as a tool for guiding admission and hiring decisions.[52] Beyond what we ourselves are putting on the Internet, data brokers are amassing every piece of information they can gather from our online habits: our locations, who we regularly contact, what we have purchased, and our sexual and political preferences.[53] And while much of this information is then sold and used to offer us products and services aligning with our preferences, many

---

49. INTERACTIVE ADVERT. BUREAU, INTERNET ADVERTISING REVENUE REPORT 6 (2021), https://s3.amazonaws.com/media.mediapost.com/uploads/InternetAdvertisingRevenueReportApril2021.pdf [http://perma.cc/RX2F-JSCY].

50. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 437 (2014).

51. *Id.* at 449.

52. *See, e.g.*, Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. TIMES (Nov. 9, 2013), https://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html [https://perma.cc/T366-BXQW]; *see also* Russ Warner, *Beware of Legal Threats Social Networks Pose*, HUFFINGTON POST (Oct. 30, 2013), https://www.huffpost.com/entry/beware-of-legal-threats-s_b_3832632 [https://perma.cc/678K-QPWJ].

53. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 34 (2015).

companies are stockpiling this information,[54] presumably reasoning that every bit of information about us will come in handy someday to assist in furthering some monetary or advertising interest.

The collection of a seemingly infinite amount of personal information provides many avenues of possible harm. Data breaches have become commonplace in our culture, causing harm through credit card fraud and disseminating our addresses and social security numbers.[55] In addition, the unregulated storage of personal data online can lead to threats, harassment,[56] and discrimination.[57] The mere accumulation of personal data has led to countless harms[58] and will continue until companies no longer view our personal data as their own to store and use. While some contend the destruction of personal data is wasteful in the context of a modern economy,[59] the commodification of online data has strayed beyond a modern capitalist tool into a harmful and unwieldy practice destined to perpetuate more harm that outweighs the monetary value it brings to a few large companies.

III. STEPS TOWARD PROTECTING DATA PRIVACY: WHAT HAS BEEN DONE SO FAR?

A. An International Perspective

Many countries worldwide have begun to enact general personal data protection laws on a national level.[60] Notably, in 2016, the European

54. *Id.*

55. *See, e.g.*, 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/VXB2-J7SM] (breach of Target customer personal information); *Equifax Data Breach Settlement*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [https://perma.cc/ZM2C-49D6] (Equifax credit bureau data breach exposed personal information of 147 million people, led to $425 million settlement); PAUL B. LAMBERT, UNDERSTANDING THE NEW EUROPEAN DATA PROTECTION RULES 28–30 (2018) (noting that data breaches are occurring with higher frequency and scale, including two data breaches from Yahoo, affecting 500 million and 1 billion users).

56. *See* Mary Anne Franks, *Unwilling Avatars Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224 (2011). "[T]he effects of unwilling online embodiment [like harassment resulting from abuse of data] are potentially even more pernicious and long-lasting than real-life harassment" due to unique features of the Internet, including the permanence of personal information on the web and the extreme difficulty in actually deleting data from the Internet. *Id.* at 255–56.

57. Wells Fargo's home mortgages website had a "community calculator" which used the current zip code of potential customers to steer the customer to neighborhoods based on the predominant race of that zip code, which resulted in referring white people to predominantly white neighborhoods, and black people to predominantly black neighborhoods. SCHNEIER, *supra* note 53, at 109.

58. See *supra* footnotes 53–55 and accompanying text for examples of those harms.

59. *See* Edward J. McCaffery, *Must We Have the Right to Waste?*, in NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 76–81 (Stephen R. Munzer ed., 2001).

60. SAMUEL, *supra* note 29, § 15:3 (a list of personal data protection laws by country).

Union (EU) legislated the "single most important personal data and data protection set of rules to arrive in over [twenty] years."[61] The General Data Protection Regulation (GDPR)[62] places an emphasis on human rights.[63] Not only do these data protection measures give protections to the nearly 400 million estimated Internet users in the EU,[64] but they have a significant impact on companies worldwide that interact directly, or as a third party, with the EU.[65] Furthermore, unlike the United States, the EU has implemented data protection laws that are "of the highest standards in the world"[66] and provide certain protections across the entire economy.[67] The GDPR has already displayed its enforcement power by instituting hefty fines on companies for various legal violations.[68] Related to the issues arising from the unregulated collection, and often mismanagement, of personal data, the EU highlighted several benefits from the GDPR as major motivations for the extended protection, including: "Easier Access to Your Own Data," "A Right to Data Portability," "The Right to Know When Your Data Has Been Hacked," and, arguably the most relevant to this Note, "A Clarified 'Right to Be Forgotten."[69]

The right to be forgotten is an essential part of controlling one's personal data. That right gives an Internet user the ability to take back ownership of the data by acknowledging a fundamental right to destroy it. However, the Internet's mechanisms make it challenging for users to confirm they have completely deleted something online and data controllers have not retained their private information.[70] Through the right

---

61. LAMBERT, *supra* note 55, at 1.

62. *See generally* 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 O.J. (L 119) (General Data Protection Regulation) (EU) [hereinafter GDPR].

63. Samuel W. Royston, *The Right to Be Forgotten: Comparing U.S. and European Approaches*, 48 ST. MARY'S L.J. 253, 254 (2016).

64. *Internet Usage in the European Union—2021,* INTERNET WORLD STATS (Dec. 31, 2020), https://www.internetworldstats.com/stats9.htm [https://perma.cc/Z9PE-YQME]. Of those 400 million users, 250 million use the Internet every day. LAMBERT, *supra* note 55, at 37 (quoting the EU Commissioner).

65. Under these regulations, organizations are called "data controllers," and the GDPR applies to all controller and data processor organizations and "non-compliance or inadequate compliance can result in penalties of up to . . . 4% of global annual turnover." LAMBERT, *supra* note 55, at 2.

66. Peter Heim, *The Quest for Clarity on Data Protection and Security*, NETWORK SECURITY (Feb. 2014) at 8.

67. LAMBERT, *supra* note 55, at 9.

68. Jim Martin, *This Is How Much Money Facebook Earns from Your Data Each Year*, TECH ADVISOR (Jan. 28, 2022), https://www.techadvisor.com/news/security/how-much-facebook-earns-from-your-data-3812849/ [https://perma.cc/S59E-KLUK]. For example, Google paid $57.7 million for not making data processing information readily available to users, and British Airways and Marriott Hotels paid $22.9 million and $20.6 million, respectively, for data breaches. *See id.*

69. LAMBERT, *supra* note 55, at 31 (italics omitted).

70. *See, e.g.*, *Terms of Service*, *supra* note 39 and Part I.

to be forgotten, users regain control of having their information erased from the Internet by effectively destroying it and making it no longer an option for companies to trade or sell that information. The GDPR authorizes users to opt against consent to a third party's use of their data or to later withdraw consent to prevent further use of their data.[71] The GDPR conveys the following rights to users regarding the use and destruction of personal data:

> A data subject should have the right to have personal data concerning [their] rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the *right to have [their] personal data erased* and *no longer processed* where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a *data subject has withdrawn [their] consent* or objects to the processing of personal data concerning him or her, or where the processing of [their] personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given . . . consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the [I]nternet.[72]

The wording of this provision highlights the fundamental right to control a user's personal data, by functionally giving the power back in the form of revocation of consent as a tool to require data controllers to erase that information.

Furthermore, the GDPR addresses the issue of linked content to other sites by providing the "right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data."[73] This provision's impact on data privacy litigation is best highlighted in the seminal case *Google Spain Sp. v. Agencia Espanola de Proteccion de Datos*.[74] The plaintiff, Mr. Costeja Gonzalez, brought suit over the inclusion of several newspaper articles containing his name in connection with real estate auctions in Google Spain search engine results. After weighing the benefits of public access to online information against Mr.

---

71. LAMBERT, *supra* note 55, at 199.

72. General Data Protection Regulation (GDPR) 2016/679, art. 17, 2916 O.J. (L 119) (EU) (emphasis added).

73. *Id.*

74. *See generally* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, European Court of Justice ECLI:EU:C:2014:616 (May 13, 2014).

Gonzalez's right to privacy, the court ruled in favor of Mr. Gonzalez, requiring the search engine to delete those links containing his personal information from the list of Google results.[75] This court's holding required Google Spain to delete the search engine results and ultimately demonstrated the real power that the 'right to be forgotten' provision affords individuals.

B. In the United States

The United States has taken a different approach to enacting data privacy laws. In contrast to the overarching GDPR, **"**there is only a 'patchwork' of federal regulations in the United States that protect certain types of sensitive information."[76] These piecemeal federal laws include the Federal Trade Commission Act,[77] the Children's Online Privacy Protection Act,[78] and the Fair Credit Reporting Act.[79] While some states have enacted their own data privacy legislation, there are fundamental differences in their approach compared to the GDPR's.

First, while the GDPR requires "a legal basis and legitimate purpose" before companies can process data, the United States allows for commercial data to be processed unless forbidden by law.[80] In fact, United States courts have explicitly recognized this fundamental difference, stating "such a 'right to be forgotten,' although recently affirmed by the Court of Justice for the EU, is not recognized in the United States."[81] Thus, while the EU recognizes the protection of online personal data as a fundamental right, the United States does not.[82]

1. California

Given the vast extent that U.S. companies have of utilizing personal data, California was the first state to enact data privacy laws related to the use of personal data on the Internet.[83] "California, similarly to the [EU],

---

75. *Id.*

76. Sarah Shyy, *The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business,* 20 U.C. DAVIS BUS. L.J. 137, 142 (2020).

77. 15 U.S.C. § 58.

78. 15 U.S.C. § 6501.

79. 15 U.S.C. § 1601.

80. LAMBERT, *supra* note 55, at 14.

81. Garcia v. Google, Inc., 786 F.3d 733, 745 (9th Cir. 2015).

82. LAMBERT, *supra* note 55, at 14.

83. *See e.g.*, Jake Holland, *California Will Be First State with Its Own Privacy Regulator*, BLOOMBERG L. (Nov. 4, 2020), https://news.bloomberglaw.com/privacy-and-data-security/california-will-be-first-state-with-its-own-privacy-regulator [https://perma.cc/5ED7-TBQB].

has taken the view that substantive data protection regulations are essential to safeguard the rights and freedom of individuals in a democracy."[84]

In 2018, California enacted the California Consumer Privacy Act (CCPA)[85] to demonstrate that the state legislature recognized privacy as a fundamental right and the Internet's pervasiveness throughout most people's lives.[86] Geared towards providing consumers more rights regarding their personal data used by corporations, the CCPA applies to businesses earning $25 million in yearly revenue, selling 50,000 consumer records per year, or deriving 50% of its yearly income from selling personal information.[87] The bill also provides that an individual consumer may recover actual damages, or damages in the amount of $100–$750, for each incident, whichever is greater, when a business violates the provisions of the bill.[88]

Notably, a provision of the CCPA contains a "consumers right to deletion," which gives consumers the "right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[89] While this provision reads similarly to the GDPR's "right to be forgotten," the California statute provides numerous exceptions that do not require compliance by businesses to delete information. Out of the nine exceptions listed in the statute, several appear to provide extremely broad lenience to companies. For instance, among other exceptions, a business may maintain personal information to:

> 3) Debug to identify and repair errors that impair existing intended functionality. 4) Exercise free speech, ensure the right of another consumer to exercise [their] right of free speech, or exercise another right provided for by law . . . . Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research . . . [and] otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.[90]

84. Dyann Heward-Mills & Helga Turku, *California and the European Union Take the Lead in Data Protection,* 43 HASTINGS INT'L & COMP. L. REV. 319, 319 (2020).

85. CAL. CIV. CODE § 1798.100 (West 2018).

86. *See* A.B. 375, 2018 Legis. Counsel, Reg. Sess. (Ca. 2018).

87. CAL. CIV. CODE § 1798.105.

88. CAL. CIV. CODE § 1798.150.

89. CAL. CIV. CODE § 1798.105.

90. *Id.*

Additionally, when the statute goes into effect on January 1, 2023, it will only apply to data collected on or after January 1, 2022.[91] This timeframe excludes the entire first generation of Internet users, who were the least informed of the potential harms and effects of putting information online.

Perhaps sparked by the largest United States consumer population taking strides in the direction of more sufficient data privacy laws,[92] many states have begun to follow suit by implementing their own data privacy legislation, which similarly fails to provide data property protections for users.[93]

2. Virginia

In March 2021, Virginia passed SB 1392, its Consumer Data Protection Act (VCDPA), to establish a "framework for controlling and processing personal data."[94] There are several significant differences from the CCPA that align more with the European GDPR protections, including those regarding "the adoption of data protection assessment requirements, and 'controller' and 'processor' terminology."[95] Similarly, the VCDPA departs from the CCPA by leaving enforcement entirely up to the Attorney General and by not providing any private right of action for consumers when a company violates the VCDPA.[96]

While the VCDPA shares some characteristics with the GDPR, the VCDPA is stunted in the breadth of its protections: it only applies to personal data in an "individual or household context." Thus, the VCDPA does not protect personal information available within an employment or consumer context.[97] Furthermore, the definition of personal data is

---

91. Holland, *supra* note 83.

92. With 39 million residents, California represents the world's fifth largest economy by GDP. Taylor J. Wilson & Jimmy Choi, *How Does Consumer Spending Differ Among Households in California, Texas, and New York? A New BLS Data Product Can Tell Us*, U.S. BUREAU OF LAB. STAT: BEYOND THE NUMBERS (Sept. 23, 2019) https://www.bls.gov/opub/btn/volume-8/consumer-spending-ca-tx-ny.htm [https://perma.cc/V65J-BLD7].

93. Wharton University of Pennsylvania, *Your Data Is Shared and Sold . . . What's Being Done About It?* KNOWLEDGE @ATWHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/NJ35-T9YR]. Lacking a federal legislative response to data privacy measures inspired by state action, further data privacy piecemeal legislation has the very likely effect of causing great impact on business productivity in the context of operating on a worldwide platform.

94. S.B. 1392, 2021 Gen. Assemb., Reg. Sess. (Va. 2021).

95. *Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/wp-content/uploads/2021/03/virginia-passes-comprehensive-privacy-law.pdf [https://perma.cc/CXT5-NMPH].

96. *Id.*

97. Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/ [https://perma.cc/R62C-5FXZ].

extremely limited: data use compliance is exempt under the VCDPA if "a business has a reasonable basis to believe [the personal information is] lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience."[98] In effect, the VCDPA lends no data privacy protections to information posted on any social media channel or other online platform.[99] Similar to the CCPA, the VCDPA purports to honor the data privacy rights of users, while simultaneously implementing enough loopholes for businesses to continue to profit from the accumulation of personal data and the removal of a private right of action for individuals to seek remedy. While California and Virginia have moved closer to a digital landscape where personal data is prioritized over business gains, the new legislation has not gone far enough.

IV. WASHINGTON STATE'S PROPOSED LEGISLATION AND WHY IT DOES NOT GO FAR ENOUGH

Other states' data privacy bills lack individual protections, and Washington State's proposed data privacy legislation is no exception. Washington State has included a data privacy bill on its docket for several years but has yet to pass legislation in this area. The most recent version in the Washington legislature is SB 5062, otherwise known as the Washington Privacy Act, concerning the management, oversight, and use of data.[100] So far, all iterations of the bill include a right to access (confirmation of whether an entity—a "controller"—is processing your personal data); a right to correction or deletion of personal data; a right to data portability (enabling consumers to obtain in a usable format their own personal data from the controller/business); and a right to opt-out, requiring businesses to discontinue processing personal information.[101]

The first issue that critics of the current version of the bill point out is the "laundry list of exemptions" as well as "a provision that explicitly prohibits people from holding companies accountable when they violate people's digital privacy rights,"[102] which renders this bill incapable of

98. *Id.*

99. *Id.*

100. S. 5062, 2021 Reg. Sess., at 1 (Wash. 2021).

101. Christopher W. Savage & Kara K. Trowell, *Focus on the Proposed Washington Privacy Act*, DAVIS WRIGHT TREMAINE LLP (Mar. 4, 2020), https://www.dwt.com/blogs/privacy—security-law-blog/2020/03/washington-privacy-act-sb-6281 [https://perma.cc/H7T8-8XET].

102. Jennifer Lee, *Con: The People's Privacy Act, Not the Washington Privacy Act, Is the Better Bill to Protect Consumers' Civil Rights and Civil Liberties*, SEATTLE TIMES (Feb. 5, 2021), https://www.seattletimes.com/opinion/con-the-peoples-privacy-act-not-the-washington-privacy-act-

requiring more accountability from companies and lacking the necessary consumer protections.[103] Also glaringly missing from the bill is a private right of action for consumers to access damages for misuse of their data.[104] In addition, while businesses must provide a copy of any data they process upon request from the consumer, they can charge "a reasonable fee based on administrative costs."[105]

Furthermore, the bill does not preempt local laws and ordinances, nor contains regulations on the commercial use of facial recognition technologies,[106] two major concerns for many privacy activists. This concern has culminated in the creation of a secondary data privacy act, the People's Privacy Act, HB 1433.[107] Apart from the fact that a competing data privacy bill from SB 5062 may cause further delays in establishing data privacy provisions for Washington residents, neither bill addresses the fundamental underpinning of effective data privacy laws: the explicit establishment of the true owner of the data, supported by a personal property right that grants control to one's own data. Without establishing a succinct definition of personal data as personal property, "[c]onsumers [will] still lack the ability to make free, informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of personal data."[108] Likewise, great challenges will arise in the actual protection of personal data because "there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity."[109]

---

is-the-better-bill-to-protect-consumers-civil-rights-and-civil-liberties/ [https://perma.cc/NYR9-T5C6].

103. *See id; see also* Jon Pincus, Aneelah Afzali & Jennifer Lee, *Washington Needs a Privacy Law That Protects People, Not Corporations*, SEATTLE TIMES (Dec. 8, 2020), https://www.seattletimes.com/opinion/washington-needs-a-privacy-law-that-protects-people-not-corporations/ [https://perma.cc/34TU-WN9K].

104. *See* Glenn A. Brown, *Washington and Oklahoma Privacy Bills Have Officially Died; Florida's Privacy Bill Is Significantly Amended*, NAT'L L. REV. (Dec. 2, 2021), https://www.natlawreview.com/article/washington-and-oklahoma-privacy-bills-have-officially-died-florida-s-privacy-bill [https://perma.cc/FSY6-2EHK]; *see also* Jim Halpert & Samantha Kersul, *The Washington Privacy Act Goes 0 For 3*, IAPP (Apr. 26, 2021), https://iapp.org/news/a/the-washington-privacy-act-goes-0-for-3/ [https://perma.cc/T8WN-4YUR].

105. S. 5062, 2021 Reg. Sess., at 12 (Wash. 2021).

106. Henry Kenyon, *Washington State Data Privacy Bill Clears Senate, Moves to House*, 2020 WL 895622.

107. *See Washington State Rep. Shelley Kloba Introduces New Data Privacy Bill: The People's Privacy Act*, ACLU WASHINGTON (Jan. 28, 2021), https://www.aclu.org/press-releases/washington-state-rep-shelley-kloba-introduces-new-data-privacy-bill-peoples-privacy [https://perma.cc/R7DA-DS49]; *see also Washington State Inches Closer to Passing Consumer Privacy Law*, BLOOMBERG L. (Mar. 4, 2021), https://news.bloomberglaw.com/privacy-and-data-security/washington-state-inches-closer-to-passing-consumer-privacy-law [https://perma.cc/5GVJ-VC8T].

108. Shyy, *supra* note 76, at 140.

109. *Id.*

A right to deletion of personal data is not enough; users will not be able to experience actual protection online unless and until legislation is passed, that extends property rights to personal information online. Furthermore, protection of data will be hindered by individual data privacy laws fractured by the state and the lack of a mechanism for verifying whether data is being deleted or amended. With Washington State poised to instate some kinds of consumer data protections extending to online commerce and our digital presence, the proposed legislation must explicitly include a provision that protects the fundamental right to destroy one's property.

One such tactic to create this protection in the legislation is to include a data expiration clause in either of the Washington bills.[110] Proposed by Viktor Mayer-Schonberger[111] with later details added by Karen Majovski, a data expiration clause would mandate all websites that allow users to post self-generated content also provide, free of charge, the requisite technology to delete expired data at a timeframe set by the user.[112] A concept like a data expiration clause ensures the Internet functions more like real life. The house that our great-grandparents grew up in is likely not still standing, a piece of graffiti will not last beyond the next century, and we do not expect our daily updates to be available to our future generations without intentional preservation measures. Treating online personas as we treat tangible possessions would "make it easier for users to erase past indiscretions, photos, and comments from the Internet."[113] A recognition of property rights over our personal data and the ability to control its distribution and destruction would allow the user the option to choose, rather than allowing companies to make, individual decisions about someone else's personal data.

CONCLUSION

The law has already acknowledged there is room for the recognition of property rights in intangible items: patent law allows for property rights in methods and processes, and trademark law allows for protection of brand names.[114] In recent years, personal data has transformed into something that one can also have a legitimate property interest in.[115]

110. Karen Majovski, *Data Expiration, Let the User Decide: Proposed Legislation for Online User-Generated Content*, 47 U.S.F. L. REV. 807, 821 (2013).

111. *See generally* MAYER-SCHONBERGER, *supra* note 37.

112. Majovski, *supra* note 110, at 818–23.

113. *Id.* at 824.

114. Determann, *supra* note 28, at 16–17.

115. *See* Glancy, *supra* note 35; *see also* Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); *ICO Warns Data Broking Industry After Issuing £80,000 Fine to Unlawful Data Supplier*, GDPR ASSOCIATES (Nov. 2, 2017), https://www.gdpr.associates/ico-warns-

Wrapped up in the immeasurably quick development of the Internet, the complete bundle of rights, including the right to exclude and ultimately to destroy, has not been afforded to the copious amounts of our data that exists in perpetuity on the Internet. With the acknowledgment that our fundamental property rights extend to our personal data, coupled with legislation that details the right to control one's own data (like a data expiration clause), individuals in Washington State will receive protection over their own personal data. Until then, many Washington citizens will continue to experience a government that prioritizes monetary goals of online businesses over protecting an individual's right to privacy.

---

data-broking-industry-after-issuing-80000-fine-to-unlawful-data-supplier/ [https://perma.cc/4LHC-RFXB] (quoting James Dipple-Johnstone, ICO Deputy Commissioner: "Businesses need to understand they don't own personal data—people do and those people have the right to know what is happening to it."); Jeffrey Ritter & Anna Mayer, *Regulating Data As Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 229 (2018) (proposed German legislation gives "data the same legal status as material commodities, to assure data can be allocated as property towards a natural person or a legal entity"). *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967) (suggesting personal information should be recognized as deserving of property rights).