2014

Online Privacy and the First Amendment: An Opt-In Approach to Data Processing

Joseph A. Tomain
Indiana University Maurer School of Law, jtomain@indiana.edu

ONLINE PRIVACY & THE FIRST AMENDMENT: AN OPT-IN APPROACH TO DATA PROCESSING

*Joseph A. Tomain**

An individual has little to no ability to prevent online commercial actors from collecting, using, or disclosing data about her. This lack of individual choice is problematic in the Big Data era because individual privacy interests are threatened by the ever increasing number of actors processing data, as well as the ever increasing amount and types of data being processed. This Article argues that online commercial actors should be required to receive an individual's opt-in consent prior to data processing as a way of protecting individual privacy. I analyze whether an opt-in requirement is constitutionally permissible under the First Amendment and conclude that an opt-in requirement is fully consistent with the First Amendment rights of data processors.

---

* Joseph A. Tomain previously served as an Associate Professor at Florida Coastal School of Law and a Visiting Assistant Professor at the University of Louisville Brandeis School of Law. Thank you to Eric Goldman and everyone at the 2013 Santa Clara Law Internet Law Work-in-Progress conference, Alexander Tsesis and everyone at the 2013 Loyola University Chicago School of Law Constitutional Law Colloquium, Megan Binder, Brian J. Foley, Susannah P. Mroz, and Joseph P. Tomain for their comments and assistance on this Article. All errors are mine.

"The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[1] – Justice Anthony Kennedy

I. INTRODUCTION

People have become the product.[2] Online commercial actors collect, use, and disclose data about individuals for financial gain, often

1. Sorrell v. IMS Health, 131 S. Ct. 2653, 2672 (2011).

2. Julia Angwin, *Has Privacy Become a Luxury Good?*, N.Y. TIMES, Mar. 4, 2014, at A23 ("if you aren't paying for the product, you *are* the product") (emphasis in original); Ryan Calo, *Digital Market Manipulation*, 42 GEO. WASH. L. REV. 995, 1047 (2014) (suggesting that through law or best practices individuals could pay a fee to opt-out of the "marketing ecosystem" and that "such an arrangement could reorient the consumer from being a product to being a client."). *See also* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 434 (2014) ("Once divulged on the Internet, private facts about persons' preferences, aversions, job and shopping patterns, and plans are commodifiable at the initiative of profit seeking corporations with sophisticated business models designed to convert mundane and intimate data, alike, into marketing strategies."); *In re* Google, Inc. Privacy Policy Litig., 2013 WL 6248499, *1 (N.D. Cal. Dec. 3, 2013) (describing Google's advertising business model as one where "the users are the real product."); Erin Bernstein & Theresa J. Lee, *Where the Consumer is the Commodity: The Difficulty with the Current Definition of Commercial Speech*, 2013 MICH. ST. L. REV. 39, 40–41 (2013); Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1246–48 (2002) ("Really astute cyberlords, however, can accomplish even more by turning their users' personalities into sources of revenue. . . . Like feudal serfs, 'cyberserfs' live 'cyberlives' managed by their lord for the lord's financial gain. As such, the cyberserf becomes an asset owned by the cyberlord's business."). Some commenters, however, take issue with a similar metaphor. *See, e.g.*, Mike Mansick, *Stop Saying 'If You're Not Paying, You're the Product*, TECHDIRT, (Dec. 20, 2012), http://www.techdirt.com/articles/20121219/18272921446/stop-saying-if-youre-not-paying-youre-product.shtml. While similar to "people have become the product," the metaphor Mansick critiques is materially different. One becomes the product through the aggregation of data and the creation of detailed profiles, regardless of whether one pays for an online service.

resulting in detailed profiles of millions of individuals. Through online behavioral advertising,[3] these profiles are used to sell products and services to the individuals themselves, their friends and family, and others with similar profiles.[4] Sometimes, these profiles are used to deny individuals access to products, services or employment, or to charge higher prices.[5] Profiling individuals and data collection occurred prior to the digital age.[6] What makes online data processing and behavioral advertising unique, however, is the exponential increase in the amount and types of data collected, and the number of actors engaged in such commercial activities, mostly without the consent of individuals whose data is being processed.[7] There is no end in sight to the proliferation of data processing and the number of actors involved, or to the development of increasingly intrusive and opaque techniques used to gather more and more data.[8] The Big Data era is just beginning.[9]

Currently, individuals have little to no choice in being commodified for firms' financial gain or preventing the concomitant privacy invasions that profiling entails. These privacy invasions by Big Data actors, such as Google, Facebook, and Acxiom, harm individuals' dignity and

---

3. Online behavioral advertising involves the long term tracking of an individual's online activity to create a detailed profile about the individual for purposes of making decisions about what kind of advertisement to display to the individual. *See infra* Part II.

4. JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH 94, 147–48 (2011) (noting that online behavioral advertising is used not only to target the individual, but also the individual's friends); Emily Steel, *Marketers Watch as Friends Interact Online*, WALL ST. J. (Apr. 15, 2010), http://online.wsj.com/news/articles/SB10001424052702304159304575184270077115444 ("in the Internet age, a customer's friend is a potential customer.") [*hereinafter* TUROW, THE DAILY YOU].

5. Michael Fertik, *The Rich See a Different Internet to the Poor*, SCIENTIFIC AMERICAN (Feb. 18, 2013), http://www.scientificamerican.com/article.cfm?id=rich-see-different-internet-than-the-poor; Pam Dixon & Robert Gellman, *The Scoring of America: How Secret Consumer Sores Threaten Your Privacy and Your Future*, WORLD PRIVACY FORUM (Apr. 2, 2014), http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

6. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000) [*hereinafter* Cohen, *Examined Lives*]; Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012, at BU1.

7. Cohen, *Examined Lives*, *supra* note 6, at 1374.

8. For example, cookies are being replaced by fingerprinting, a more sophisticated and more intrusive tracking technique. Fingerprinting "allows a web site to look at the characteristics of a computer such as what plugins and software you have installed, the size of the screen, the time zone, fonts and other features of any particular machine. These form a unique signature just like random skin patterns on a finger." Adam Tanner, *The Web Cookies is Dying. The Creepier Technology That Comes Next*, FORBES (June 17, 2013), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/.

9. VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA 103, 156 (2013) (noting that the use of Big Data is not yet commonplace); TUROW, THE DAILY YOU, *supra* note 4, at 1 ("We're at the start of a revolution in the ways marketers and media intrude in—and shape—our lives.").

autonomy interests.[10] They also harm the collective good and the democratic process.[11]

In the context of online commercial data processing generally, with a particular focus on online behavioral advertising as one example of data processing, this Article seeks to help restore the proper balance between competing interests. On the one hand are considerations of individual privacy, autonomy, dignity, and democratic participation interests. On the other hand are the financial interests of private firms. This Article contends that an opt-in regime, which would require online commercial actors to receive an individual's express, affirmative and informed consent before engaging in data processing, is a necessary part of the solution to help restore that balance. For example, before Google uses the content of an individual's email for purposes beyond sending the email to the intended recipient, Google must first receive the sender's opt-in consent for secondary uses, such as using the content of the email to target advertising at the individual or create a profile about her.[12]

Part II explains why online data processing by commercial actors is an example of cyberspace exceptionalism. Part III provides context on privacy interests and theories relevant to data processing, and shows how a law and economics analysis supports regulation of online data processing. Part IV discusses existing and proposed opt-in laws and policy in the online privacy context, including Federal Trade Commission reports and actions, White House reports, and the European Union's recently proposed General Data Protection Regulation.

Part V, the heart of this Article, analyzes the constitutionality of an opt-in requirement. Specifically, it analyzes the viability of an opt-in

---

10. *See* TUROW, THE DAILY YOU, *supra* note 4, at 7 ("[W]hen companies track people without their knowledge, sell their data without letting them know what they are doing or securing their permission, and then use those data to decide which of those people are targets or waste, we have a serious social problem."); OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *infra* note 16, at 10 ("Some of the most profound challenges revealed during this review concern how big data analytics may lead to disparate inequitable treatment, particularly of disadvantaged groups, or create such an opaque decisions-making environment that individual autonomy is lost in an impenetrable set of algorithms.").

11. Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1905 (2013) ("freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems."); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1610–18 (1999) ("cyberspace has a tremendous potential to revitalize democratic self-governance . . . [but] [i]n the absence of strong privacy rules, cyberspaces civic potential will never be attained.").

12. Jerry Kang used the phrase "functionally necessary use" to describe limiting the use of data to the underlying purpose of the transaction. Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1249 (1998). Mayer-Schoneberger and Cukier, however, believe that limiting the use of data to the original purpose is not a workable solution in the Big Data era because the main value in such data lies in secondary uses, including some that have not yet been imagined. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 153.

requirement under the commercial speech doctrine; and, it draws an analogy to a 2012 U.S. Supreme Court case that held an opt-in regime to be constitutionally required in the context of First Amendment rights of non-union member public employees.[13] The Article concludes that an opt-in requirement helps guide the law back to its intended purpose: protecting individual rights and liberties.

The point of this Article is not to deride the Big Data era in toto, as it brings substantial benefits that do not involve privacy concerns of individuals or democratic concerns of the collective whole.[14] Rather, the intent is to contribute to the scholarship seeking to create a better balance between the financial interests of online commercial data processors and fundamental human interests in privacy. An opt-in requirement may not be sufficient to protect privacy and democratic interests, but it is an important part of the solution. Requiring online commercial actors to receive an individual's express, affirmative, and informed consent would "nudge"[15] the law and society back to a focus on the interests of individuals and, could help improve our democratic process.

II. ONLINE DATA PROCESSING AND CYBERSPACE EXCEPTIONALISM

Data collection is growing increasingly ubiquitous as society moves toward the "Internet of Things"[16] where people are being tracked by a

---

13. Knox v. SEIU, 132 S. Ct. 2277, 2295–96 (2012).

14. One example of such benefits is the use of Big Data to more accurately predict the causes of manhole cover explosions. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 152. For other examples, see OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *infra* note 16, at 2.

15. *See generally*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009). While Thaler and Sunstein popularized use of the term "nudge" to describe the use of legal rules in a libertarian paternalistic way to guide people towards wise choices, people have been nudged for a long time, and not always for the good of the order. Commercial actors have been nudging individuals for their financial benefit for a long time. VANCE PACKARD, THE HIDDEN PERSUADERS 214 (2007 ed.) ("The disturbing Orwellian configurations of the world toward which the persuader seem to be nudging us – even if unwittingly – can be seen most clearly in some of their bolder more imaginative efforts."); Calo, *Digital Market Manipulation*, *supra* note 2, at 1001 ("Market manipulation is, essentially, nudging for profit.").

16. A May 2014 report from the Executive Office of the President provides the following description:

> The "Internet of Things" is a term used to describe the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks. These devices could include your thermostat your car, or a pill you swallow so the doctor can monitor the health of your digestive tract. These connected devices use the Internet to transmit, compile, and analyze data.

EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2 (May 1, 2014) [*hereinafter* OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES]; Debra Donston-Miller, *The Internet of Things Poses New Security Challenges*, FORBES (Feb. 25, 2014),

variety of devices, including their own cars[17] and cell phones.[18] "[B]ig data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more."[19] The Big Data era is possible due to the increased ability to "datify," and then monetize, information.[20] Due the growing pervasiveness of Big Data, the opt-in requirement proposed here is intended to apply to all types of data processing by all types commercial actors, including data brokers, advertising organizations, and individual companies.[21] Online behavioral advertising is used as one example of data processing because of its prevalent use by online commercial actors and because it illustrates how data profiles can be used to the detriment of individuals.

"Data processing" refers to the collection, use, sale, and disclosure of data.[22] Disclosure of data could be disclosed to a third-party, or within

---

http://www.forbes.com/sites/sungardas/2014/02/25/the-internet-of-things-poses-new-security-challenges/. *See also,* MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 173 (drawing a distinction between the Internet age and the Big Data era).

17. Jacyln Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. TIMES, Jan. 11, 2014, at B1.

18. Peter Maas & Megha Rajagopalan, *That's No Phone. That's My Tracker*, N.Y. TIMES, July 15, 2012, at SR5.

19. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 6; OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16 (noting that there are various definitions of Big Data, but that "[m]ost definitions reflect the growing technological ability to capture aggregate, and process an ever-greater volume, velocity, and variety of data.").

20. Mayer-Schonberger and Cukier define "datafication" as:

> taking information about all things under the sun—including one we never used to think of as information at all, such as a person's location, the vibrations of an engine, or the stress on a bridge—and transforming it into a data format to make it quantified. This allows us to use the information in new ways, such as in predictive analysis[.]

MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 15.

21. This approach is consistent with a 2012 recommendation that a Do Not Track system should apply broadly to all data processing. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICY MAKERS 53 (2012) [*hereinafter* FTC, RAPID CHANGE] ("an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction").

22. The European Parliament's recently proposed General Data Protection Regulation provides the following definition:

> "processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction[.]

European Parliament, General Data Protection Regulation, Comp. Art 4(3) (version Oct. 11, 2013) [*hereinafter* EU GDPR].

an integrated company, such as when Google combines an individual's video viewing activities on YouTube with content that she sends or receives via Gmail. Data processing often results in profiling individuals. Profiling is used to make predictions about individuals based on statistics and inferences.[23] One main purpose of data processing and the resulting profiles is to engage in online behavioral advertising.

Advertising can be divided into the categories of run-of-network advertising, contextual advertising, and behavioral advertising.[24] This Article is focused specifically on the online behavioral advertising category because it raises heightened privacy concerns.[25] Run-of-network advertising describes widespread advertising, regardless of context and without profiling individuals.[26] Publishing the same advertisement on all of the broadcast networks in prime time is a classic example of run-of-network advertising and for a time was extremely effective in reaching a mass audience.[27] At the other end of the spectrum is online behavioral advertising, which can be defined as "large-scale and long-term collection, storage, analysis and, in some cases, sharing of data about Internet users."[28] Contextual advertising is

---

23. The recently proposed General Data Protection Regulation of the European Parliament provides the following definition: "'profiling' means any form of automated processing of personal data intended to evaluate certain aspects relating to a natural person or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior." EU GDPR, Comp. Art. 4(3)(a) (version Oct. 11, 2013).

24. Katherine J. Standburg, *Free Fall: The Online Market's Consumer Preference Disconnect* 99 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2323961 [*hereinafter* Strandburg, *Free Fall*].

25. Marvin Ammori & Luke Pelican, *Media Diversity & Online Advertising*, 76 ALB. L. REV. 665, 681 (2013) ("One of the main concerns is the use of users' information for behavioral, rather than contextual, advertising.") [*hereinafter* Ammori & Pelican, *Media Diversity*].

26. Strandburg, *Free Fall*, *supra* note 24.

27. TUROW, THE DAILY YOU, *supra* note 4, at 162 ("From the mid-1960s through the mid-1980s it was possible to place commercials on CBS, NBC, and ABC in the evening – prime time – and reach around 90 percent of all households in American with their sets on. That typically translated to more than 60 percent of all homes."). Due to the rise of cable, satellite, and broadband, "commercials on those three still-major networks reach only about 30 percent of households during a typical prime-time period," not to mention technology that allows viewers to fast forward through commercials. *Id.*

28. Strandburg, *Free Fall*, *supra* note 24, at 100. There are other definitions of "online behavioral advertising." In 2009, the FTC described online behavioral advertising as "the tracking of consumers' online activities in order to deliver tailored advertising. . . . [A] practice, which is typically invisible to consumers . . ." FED. TRADE COMM'N STAFF REPORT, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009) [*hereinafter* FTC, SELF-REGULATORY PRINCIPLES]. An industry report defined online behavioral advertising as:

> the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.

a category between run-of-network and behavioral advertising.

An industry report defined contextual advertising as the delivery of "advertisements based on the content of a Web page, a search query, or a user's contemporaneous behavior on the Web site."[29] Two examples of contextual advertising help distinguish it from behavioral advertising. First, a ticket broker that places an ad on a sports-related website is an example of contextual advertising because the ticket broker is targeting a sports audience. A second example is when someone runs a search for Hawaiian vacations and an algorithm generates an advertisement for flights to Hawaii next to the search results. The critical difference between this example of contextual advertising and behavioral advertising is that the Hawaiian vacation ad is generated based on one, isolated search; whereas behavioral advertising is based on long-term and large-scale data collection.[30] The former is significantly less problematic than the latter because it is not based on nor results in a profile of an individual.[31] It is based on merely one search. Interestingly, at least one study suggests that this type of contextual advertising is more effective than behavioral advertising.[32]

A. Online Data Processing Is Exceptional

Since the mid-1990s, there has been a debate about whether cyberlaw is an independent field of study or whether laws involving cyberspace

---

AM. ASSOC. OF ADVERTISING AGENCIES, ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf [*hereinafter* AAAA, SELF-REGULATORY PRINCIPLES]. This report expressly excludes the collection and use of data by a website for its own uses from the definition. *Id.* Excluding "first-party" online behavioral advertising is too narrow, especially considering sharing that occurs within an integrated company, such as Google. The Center for Democracy and Technology subsequently published a report critiquing the industry's definition of behavioral advertising as too narrow. CENTER FOR DEMOCRACY AND TECHNOLOGY, ONLINE BEHAVIORAL ADVERTISING: INDUSTRY'S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS 8–13 (2009), *available at* https://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf [*hereinafter* CDT, INSUFFICIENT SELF-REGULATORY FRAMEWORK].

29. *Id.* at 8.

30. Strandburg, *Free Fall*, *supra* note 24, at 6–7.

31. At least some privacy advocates agree that contextual advertising is less problematic than behavioral advertising. CDT, INSUFFICIENT SELF-REGULATORY FRAMEWORK, *supra* note 28, at 8 ("CDT believes that contextual advertising . . . poses fewer privacy risks and better aligns with consumer expectations about how data is being collected and used and therefore may need a different set of protections.").

32. *See generally* Jun Yan, et al., *How Much Can Behavioral Targeting Help Online Advertising?*, 18TH INT. WORLD WIDE WEB CONFERENCE (2009), *available at* http://www.wwwconference.org/www2009/proceedings/pdf/p261.pdf. Strandburg notes that this study is often cited to show the value of behavioral advertising, but that the study is more accurately described as showing the benefits of contextual advertising or "short term" behavioral advertising. Strandburg, *Free Fall*, *supra* note 24, at 11–12.

can be analyzed in the context of the specific area of law involved, such as studying online contract formation in a Contracts course, as opposed to a standalone Cyberlaw course.[33] Over a decade ago, David Post framed the debate as one between unexceptionalism and exceptionalism, and explained why laws affecting cyberspace often deserve their own consideration.[34] This Article concurs with Post's exceptionalist analysis, which, in turn, supports an argument for an opt-in regime.

An unexceptional view is that cyberspace is no different than real physical space and reliance on existing laws for the regulation of cyberspace is sufficient.[35] An exceptional view is that there is something unique about cyberspace that calls for independent inquiry. Post believes that some interactions in cyberspace are not functionally identical to interactions in real space.[36] While smoke signals and online message boards are both used to communicate, they are not functionally identical methods of communication. While cannon balls and nuclear bombs are both weapons, they are not functionally identical in scope of harm. "Scale matters."[37] So do network effects.[38]

Neither data processing nor profiling individuals by commercial actors are unique to cyberspace. Axciom, a marketing company,[39] has collected data and created profiles on individuals for over forty years.[40] In 1957, Vance Packard detailed the lengths to which commercial actors went in order to improve the effectiveness of their advertising through "depth manipulation."[41] Neither online data collection nor profiling, however, is functionally identical to offline data collection or the "primitive" targeting techniques described by Packard.[42] Consequently, online data processing generally and behavioral advertising specifically are exceptional.[43] Indeed, there are several ways that online data

33. *Compare* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 201 (1996) *with* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

34. David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365 (2002). One does not need to be either exceptionalist or unexceptionalist in all instances. Context matters. Sometimes offline laws neatly map onto the online world. Sometimes they do not. In either case, the study of Cyberlaw allows us to engage in the inquiry.

35. *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

36. *See generally* Post, *Against "Against Cyberanarchy,"supra* note 33.

37. *Id.* at 1377.

38. DAVID EASLEY & JON KLEINBERG, NETWORKS, CROWDS, AND MARKETS: REASONING ABOUT A HIGHLY CONNECTED WORLD, 509–542 (2010).

39. AXCIOM, http://acxiom.com/ (last visited Oct. 1, 2014).

40. Singer, *Mapping, and Sharing, the Consumer Genome*, *supra* note 6.

41. PACKARD, THE HIDDEN PERSUADERS, *supra* note 15, at 31-36.

42. Tsesis, *Indefinite Retention of Data* , *supra* note 2, at 444 ("An ISP–like America Online and EarthLink–can consolidate more information about users than their families and closest friends know and even more than the subject may even remember.").

43. Calo, *Digital Market Manipulation*, *supra* note 2, at 1003 ("this new combination of

processing in this new era presents unique problems.

First, scale matters. Due to quickly developing technology, data processing occurs at an "unprecedented scale."[44] Second, the exponential increase in the scale of data processing is more than a quantitative change; it results in qualitative changes.[45] Ryan Calo noted that Big Data provides data processors with the new ability to influence individuals through the use of highly personalized messaging in ways that the "depth manipulators" of Packard's era could only dream.[46] Katherine Strandburg highlighted two other qualitative changes resulting from online data collection: interconnectedness and impenetrability.[47]

Interconnectedness means that user data does not rest in the hands of a single actor. Network effects matter. The ability to share that data among multiple actors in the Big Data era is dramatically distinguishable from past sharing capabilities. Databases are interconnected, data is sold to third-parties, and data is shared among integrated companies, such as Google search, Gmail, and YouTube.[48] The web browser, Firefox, helps illuminate the problem of interconnectedness through its add-on feature, Lightbeam (formerly known as Collusion). Lightbeam illustrates how user information from a website that a user visits is shared with third-party sites, including sites a user does not visit.[49] For example, I am not on Facebook, but Facebook is on me. In other words, several websites I visit share information about me with Facebook. Unfortunately, Lightbeam does not indicate what information is shared, which segues into Strandburg's second exceptionalist observation: impenetrability.

A user would have a difficult, if not impossible, time determining

---

interpersonal manipulation with large-scale data presents a novel challenge to consumers and regulators alike.").

44. EU GDPR, *supra* note 22, at Comp. Art 1, Recital 5; Jeff Sovern, *Opting In, Opting Out, or Not Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1033–40 (1999) [*hereinafter* Sovern, *Opting In, Opting Out*] (providing several examples of the types of databases that exist and the information that is available on individuals); Daniel Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 970 (2003) (*hereinafter*, Solove, *Virtues of Knowing Less*).

45. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 6.

46. Calo, *Digital Market Manipulation*, *supra* note 2, at 999 ("digitization of commerce dramatically alters the capacity of firms to influence consumers at personal level.").

47. Standburg, *Free Fall*, *supra* note 24, at 72.

48. TUROW, THE DAILY YOU, *supra* note 4, at 73 ("Some publishers . . . purchase data about their registrants from information vendors such as Experian and Acxiom and append them to their files.").

49. "Lightbeam is a Firefox add-on that enables you to see the first and third party sites you interact with on the Web. Using interactive visualizations, Lightbeam shows you the relationships between these third parties and the sites you visit." *Lightbeam for Firefox*, MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/lightbeam/ (last visited Oct. 1, 2014).

how her data has been, collected, used or shared among various companies because firms do not willingly reveal such information.[50] While there are legitimate business reasons to keep information secret, such as protecting trade secrets, there is also the "creepiness" factor: firms do not want users to know exactly how much information is collected, used, and disclosed because many individuals would be creeped out.[51] Individuals involved in consumer transactions or personal interactions are not the only ones creeped out. Both major party presidential campaigns engaged in data collection "behind the scenes" because they did not want voters to "get creeped out."[52] Similarly, physicians are sometimes creeped out by what information pharmaceutical sales representatives possess and use to promote their companies' drugs to prescribing physicians.[53] An opt-in regime is one way to break through the impenetrability because it would require disclosure of data processing practices and require data processors to honor an individual's choice to avoid being subject to data processing.

Third, the use of predictive analysis through algorithms creates the

---

50. TUROW, THE DAILY YOU, *supra* note 4, at 1 ("At the start of the twenty-first century, the advertising industry is guiding one of history's most massive stealth efforts in social profiling."); Richard M. Smith, *The Web Bug FAQ*, ELECTRONIC FRONTIER FOUNDATION (Nov. 11, 1999), http://w2.eff.org/Privacy/Marketing/web_bug.html (Web "bugs" are invisible "[t]o hide the fact that monitoring is taking place.").

51. *See* TUROW, THE DAILY YOU, *supra* note 4, at 7 ("*creeped out* is phrase people often use when they learn about" data processing activities) (emphasis in original), 94 (Team Detroit executive vice-president Scott Lang describing targeting Facebook friends by indicating their friend liked a car as "creepy in the beginning, but . . . they slowly get used to it"), 124 (a group manager for Microsoft's Bing News stating that automated personalization of news used in a "visible way would be creepy, many believe"); Tanner, *The Web Cookies is Dying, supra* note 8. In describing the lengths to which Target seeks to hide its data processing practices to avoid creeping out its targets, one Target executive told a reporter:

> "With the pregnancy products, though, we learned that some women react badly," the executive said. "Then we started mixing in all these ads for things we knew pregnant women would never buy, so the baby ads looked random. We'd put an ad for a lawn mower next to diapers. We'd put a coupon for wineglasses next to infant clothes. That way, it looked like all the products were chosen by chance."
>
> "And we found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons. She just assumes that everyone else on her block got the same mailer for diapers and cribs. As long as we don't spook her, it works."

Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

52. Kashmir Hill, *The Obama And Romney Campaigns Know If You've Visited Porn Sites. Why 'Do Not Track' Matters*, FORBES (Oct. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/10/16/the-obama-and-romney-campaigns-know-if-youve-visited-porn-sites-why-do-not-track-matters/.

53. Katie Thomas, *Glaxo Says It Will Stop Paying Doctors to Promote Drugs*, N.Y. TIMES, Dec. 17, 2013, at A1 ("'As a physician, I periodically meet with these sales reps and they usually come in armed with information about me that I don't even know,' he said, like the number of prescriptions he writes for the drug company's product. 'I feel that's not really a comfortable interaction to have.'").

risk of replacing judgment based on actions with judgment based on probable propensities.[54] There is no dispute that such predictive analysis occurs. An industry created definition of online behavioral advertising expressly states that the purpose of such data processing is "to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors."[55] The use of such statistical inferences to profile individuals will affect the advertisements one is shown or discounts offered.[56] Many consumers will welcome this activity because it provides them with useful information and lowers their search costs. But, there are also costs to individuals. An opt-in allows an individual to choose whether the benefits are worth the costs. At this time, individuals do not have such a choice.

Fourth, Big Data makes prior legal and technical means used to protect privacy ineffective.[57] Several commentators state that reliance on notice and consent mechanisms do not work well to protect online privacy.[58] Notice and consent regimes do not work effectively enough, in part, because privacy policies are notoriously vague and broad.[59] One reason that privacy policies are vague and broad is because the current default is that an individual has to opt-out of data processing, if there is such an option at all, and a firm has natural business incentives to prevent the individual from opting-out: firms want data on as many individuals as possible.[60] Another reason that notice and consent regimes do not work effectively enough is that contract terms and

---

54. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 151.

55. AAAA, SELF-REGULATORY PRINCIPLES, *supra* note 28, at 1.

56. TUROW, DAILY YOU, *supra* note 4, at 158; OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 46.

57. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 192 ("[Big data] renders ineffective the core technical and legal mechanisms through which we currently try to protect privacy.").

58. Strandburg, *Free Fall*, *supra* note 24, at 69. ("The behavioral advertising business model gives companies an insatiable thirst for personal information and drives them to obfuscate the extent of data collection from consumers. Those imperatives cannot be avoided by improving 'notice and choice' or even by more robust consent regimes); Tsesis, *Indefinite Retention of Data* , *supra* note 2, at 433 ("The concept of informed consent is often misleading on websites with policies that are written for lawyers and difficult to understand by ordinary Internet users."); *but see* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012); Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013) (Ohm suggests requiring a company to change their brand image to signal significant changes in its privacy policy as a form of notice to users).

59. Strandburg, *Free Fall*, *supra* note 24, at 57 ("Privacy policies are notoriously ineffective at providing information to consumers about online businesses' data practices.").

60. Sovern, *Opting In, Opting Out*, *supra* note 44, at 1105; TUROW, DAILY YOU, *supra* note 4, at 87 (website owners are incentivized to "create privacy policies to hide particulars of [data] buyers' audience-tracking and targeting activities from visitors to their sites); Strandburg, *Free Fall*, *supra* note 24, at 61 ("Companies have every incentive to keep these transaction costs high in order to discourage consumers from taking steps to avoid data collection."). Price discrimination is a specific example of information that firms naturally would not want to share with individuals. *Id.* at 58.

privacy polices often go unread.[61] Although some individual responsibility and accountability is warranted, there are limits to the persuasiveness of the argument that individuals lack information about a company's data processing practices because of indifference.[62] Even if the scope of contracts one enters into is limited to online privacy policies, one study concluded that it would take an average of 201 hours per year for an individual to read the privacy policies of all the websites she visited in a year.[63]

Not only do existing legal mechanisms fail to protect privacy from online data processing, existing technical mechanisms are also inadequate. One example is the "broken promise" of anonymity.[64] Studies have shown that is relatively easy to re-identify or de-anonymize a user with very few inputs.[65] Additionally, anonymous data can easily be revealed by enticing an individual to provide identifying information to participate in activities, such as sweepstakes.[66] Thus, anonymization cannot be relied upon to protect online privacy because it is technically ineffective.[67] Because of the ease with which anonymous data can be de-anonymized, the distinction between "personally identifiable information" and "non-personally identifiable information" as a basis to protect privacy is not workable.[68] It is important to note, however, that technical mechanisms can be part of the solution to protecting privacy from online data processing.[69]

Striking a balance between individual privacy and the financial

---

61. This informed consent problem is not exceptional to cyberspace. *E.g.*, MARGRET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013).

62. Strandburg, *Free Fall*, *supra* note 24, at 56 ("It is unreasonable to conclude that a consumer's lack of information results from indifference.").

63. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. OF L. & POL'Y FOR THE INFO. SOC'Y 543, 562 (2008). "Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually." *Id.*

64. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

65. *Id.* at Part I.A.1.3 and n.4 (*citing* Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population (Laboratory for Int'l Data Privacy*, Working Paper LIDAP-WP4, 2000); Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y 77, 78 (2006)).

66. TUROW, DAILY YOU, *supra* note 4, at 100.

67. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 154; OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 8.

68. *See generally* Ohm, *Broken Promises*, *supra* note 64.

69. Although existing technical mechanisms are ineffective, that is not a reason to abandon use of technical mechanisms as part of the solution for protecting individuals' privacy from online data processing. *See, e.g.*, Nick Bilton, *Disruptions: Internet's Sad Legacy: No More Secrets*, N.Y. TIMES, Dec. 16, 2013, at B8 ("This may be one of those once-in-a-generation moments when we recalibrate the powers of the citizens and the state. . . . . And that change can happen on the technological side, where the technologists that are disillusioned by the incessant tracking will use their skills to make surveillance more costly.").

interests of commercial actors is not a new problem.[70] The examples above, however, help show that the Big Data era has fundamentally changed our society in exceptional ways. While these technological developments have provided financial benefits to commercial actors,[71] these financial benefits come at the expense individual privacy interests.[72] Further, these technological developments have also made existing legal mechanisms for protecting privacy ineffective, which demands new legal responses. Of course, this is not the first time that technological development has disrupted existing legal regimes.

"Just as the printing press prepared the ground for laws guaranteeing free speech—which didn't exist earlier because there was so little written expression to protect—the age of big data will require new rules to safeguard the sanctity of the individual."[73] This insight shows that we cannot rely on existing laws to protect fundamental privacy interests, just as we could not rely on existing laws to protect freedom of expression after the printing press created a dramatic increase in the amount of written expression. At that time, new laws were necessary to protect against censorship and patronage[74] because those restrictions threatened individuals' dignity interests in free expression. At this time, new laws are necessary to protect fundamental privacy interests that online data processing threatens.[75]

The use of probabilities and algorithms threaten one's access to mortgage loans, health care, or employment.[76] Additionally, the use of online data processing threatens to undermine intangible interests unique to human beings by the commodification of humanity. For these

---

70. *E.g.*, PACKARD, HIDDEN PERSUADERS, *supra* note 15, at 240 ("The most serious offense many of the depth manipulators commit . . . is that they try to invade the privacy of our minds.").

71. In two years, Google went from zero to $2.08 billion from advertisements appearing next to search results. TUROW, DAILY YOU, *supra* note 4, at 65.

72. To be sure, Big Data has public interest benefits as well. *See generally* MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9; Jane Yakowitz (n/k/a Jane Bambauer), *Tragedy of the Data Commons*, 25 HARV. J.L. TECH. 1 (2011). These public interest benefits are worth protecting, but are beyond the scope of this Article. The solution proposed here seeks to avoid disrupting the public interest benefits that big data can provide by focusing on commercial data processing.

73. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 17.

74. For further information on literary patronage, *see generally* DUSTIN GRIFFIN, LITERARY PATRONAGE IN ENGLAND 1650–1800 (1996).

75. For example, to protect privacy interests in the Big Data era, the law must reconceptualize when information is "private," even though third-parties possess the information. Shaun Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S. CAR. L. REV. 373 (2013). Spencer notes that existing law often finds that an individual does not have a protectable privacy interest when the information is possessed by a third-party. He advocates for a contextual, as opposed to a binary, conception of privacy because the binary conception of privacy: (1) "ignores the difference between sharing with third parties as ends and sharing with third parties as means;" (2) "ignores the anti-aggregation norm—our deep seated aversion to mass surveillance;" and (3) "rests upon a flawed assumption of consent." *Id* at 401.

76. MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 17.

reasons and others, this Article asserts that meaningful consent is required before online commercial actors engage in data processing. An opt-in consent mechanism is a necessary condition to help restore a proper respect for fundamentally humanistic interests.[77] An opt-in requirement is a necessary part of the solution because it helps restore the primacy of individual privacy interests in the Big Data era. Before further analysis of the opt-in requirement, some elaboration on the privacy interests at stake is necessary because privacy itself is an unsettled concept.

III. PRIVACY

Compared to other areas of law, such as contracts and torts, privacy law is "relatively young."[78] The roots of American privacy law are generally attributed to Samuel D. Warren's and Louis D. Brandeis' 1890 article, *The Right to Privacy*.[79] A singular definition of privacy continues to elude commentators.[80] Perhaps there will never be a singular definition because "[p]rivacy is a chameleon that shifts meaning depending on context"[81] and contexts continually change. Nevertheless, we can identify privacy interests involved in the context of commercial data processing generally and behavioral advertising specifically.

A. Privacy Interests and Theory

Several commentators believe that privacy determinations must be contextual.[82] Under the rules of evidence for example, the same piece

77. *Cf.* PACKARD, HIDDEN PERSUADERS, *supra* note 15, at 34 ("All this probing and manipulation has . . . seriously antihumanistic implications. Much of it seems to represent regress rather than progress for man in his long struggle to become a rational and self-guiding being.").

78. Solove, *Virtues of Knowing Less*, *supra* note 44, at 1030. Then again, perhaps like the concept of privacy itself, one's perspective of time is relative depending on the context. *See* Kang, *Information Privacy in Cyberspace Transactions*, *supra* note 12, at 1999 ("A conversation about privacy, of course, has been ongoing for a long time.").

79. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Seventy years later, William Prosser analyzed hundreds of privacy cases since the Warren and Brandeis article and created a list of four invasion of privacy torts: (1) false light; (2) public disclosure of private facts; (3) intrusion upon seclusion; and (4) misappropriation. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

80. "'Perhaps the most striking thing about the right to privacy,' philosopher Judith Jarvis Thomson has observed, 'is that nobody seems to have any very clear idea what it is.'" Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 480 (2006) (quoting Judith Jarvis Thompson, *The Right to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272 (Ferdinand David Schoeman ed., 1984)).

81. Kang, *Information Privacy in Cyberspace Transactions*, *supra* note 12, at 1202.

82. *E.g.*, NISSENBAUM, PRIVACY IN CONTEXT, *infra* note 85; SOLOVE, UNDERSTANDING

of evidence may or may not be admissible depending on the context.[83] Similarly, whether particular information receives privacy protection may depend on the context.[84] In this Article, the relevant context is an individual's informational privacy interests that are threatened by online commercial actors.[85] Informational, or data, privacy "concerns an individual's control over the processing—i.e. the acquisition, disclosure, and use—of personal information."[86] Online data processing by commercial actors affects several interests that informational privacy protects.

1. Specific Privacy Interests

Privacy is both an interest in itself, such as the right to be alone, and a proxy for protecting other interests that would be harmed without privacy protection. First, informational privacy protects the dignity interests of individual human beings. When an expert panel recommended that the Obama Administration drastically curtail the N.S.A.'s surveillance activities, it specifically cited their interest in safeguarding "the privacy and dignity of American citizens."[87] As the opening epigraph above shows, a majority of the Supreme Court also recognized that data processing creates risk to individuals' personal privacy and dignity interests. Similarly, the Charter of Fundamental Rights of the European Union expressly provides, "Everyone has the right to the protection of personal data concerning him or her."[88]

Second, informational privacy protects individual autonomy.[89] Neil Richards set forth a theory of intellectual privacy that, in part, protects individual autonomy from unwarranted intrusions.[90] An opt-in requirement directly supports the autonomy interest because the individual retains the right to choose to participate in data processing. An opt-out mechanism is insufficient due to informational asymmetry

---

PRIVACY, *infra* note 85; Kang, *Information Privacy in Cyberspace Transactions*, *supra* note 13, at 1202.

83. Solove, *Virtues of Knowing Less*, *supra* note 44, at 1031.

84. *Id.*

85. Jerry Kang described three "clusters" of privacy categories: (1) physical space; (2) decisional or choice, such as the right to choose abortion; and (3) informational privacy. Kang, *Information Privacy in Cyberspace Transactions*, *supra* note 12, at 1202–03. For other taxonomies of privacy, see, e.g., DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008); and, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009) [*hereinafter* NISSENBAUM, PRIVACY IN CONTEXT].

86. *Id.* at 1203.

87. David E. Sanger & Charlie Savage, *Obama is Urged to Sharply Curb N.S.A. Data Mining*, N.Y. TIMES, Dec. 19, 2013, at A1.

88. Charter of Fundamental Rights of the European Union, Art. 8(1), 2012 O.J. (C 326) 397.

89. Calo, *Digital Market Manipulation*, *supra* note 2, at 1024–34.

90. Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 404 (2008).

and power imbalances between individuals and private commercial actors, as well the natural financial incentive of firms to maintain these conditions.[91]

Third, informational privacy is important to more than just the individual involved. Informational privacy helps protect the democratic process. Commentators have explained how protecting informational privacy can help the democratic process.[92] President Obama's introductory letter to the 2012 White House report on *Consumer Data Privacy in A Networked World* states that privacy has been at the "heart of our democracy since its inception."[93] And, the Court has also recognized the importance of informational privacy in a democratic society.[94] Thus, there is broad consensus that privacy has a role in a functional democratic society.

Fourth, associational privacy is particularly relevant when considering online privacy.[95] Justice Sotomayor made this observation in her concurring opinion in *United State v. Jones* in the context of government surveillance where the majority held that attaching a GPS

---

91. *See* OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 39 ("While big data will be a powerful engine for economic growth and innovation, there remains the potential for a disquieting asymmetry between consumers and the companies that control information about them.").

92. *See, e.g.*, Cohen, *What Privacy is For*, *supra* note 11, at 1905; Paul Schwartz, *Privacy & Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999).

93. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf) [*hereinafter* WHITE HOUSE PRIVACY REPORT].

94. In 2001, the Court stated:

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.

Bartnicki v. Vopper, 532 U.S. 514, 533 (2001) (quoting PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967)). Although *Bartnicki* held that publication of an illegally recorded telephone conversation was protected by the First Amendment because the publisher did not participate in the illegal act and lawfully obtained the tape, the Court emphasized that the conversation involved a matter of public importance. *Id.* at 533–34. Online commercial data processing does not involve matters of public importance. Rather, it involves private information used for private financial gain. *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 761–62 (1985) (credit report is not a matter of public concern, it is "speech solely in the individual interest of the speaker and its specific business audience"); *and,* Trans Union Corp. v. F.T.C., 245 F.3d 809, 818 (D.C. Cir. 2001) ("Like the credit report in *Dun & Bradstreet* . . . the information about individual consumers and their credit performance communicated by Trans Union target marketing lists is solely of interest to the company and its business customers and related to no matter of public concern.").

95. Ammori & Pelican, *Media Diversity*, *supra* note 25, at 674; Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1377 (2012).

tracking device to an individual's vehicle without a warrant violated the Fourth Amendment.[96] Associational privacy is also intruded upon when private actors engage in data processing, such as by tracking an individual through geolocation technology or when mobile app providers have accessed users' contacts without notice.[97]

Finally, there is a qualified First Amendment right to engage in anonymous speech. *McIntyre v. Ohio Elections Commission* held that there is a First Amendment right to distribute anonymous leaflets opposing a ballot issue.[98] Relatedly, a right to read anonymously is noted as an important aspect of privacy.[99] An example of the right to read anonymously being violated by Big Data actors is the tracking of e-readers' reading activities.[100]

In short, data processing by commercial actors brings into conflict a variety of individual interests protected by informational privacy and the financial interests of artificial entities. Big data actors are aware of the individual privacy interests at stake. Indeed, some of the largest Big Data actors recently acknowledged the importance of individual privacy, at least when the government is the data processor.

2. Data Processors Acknowledge Individuals' Privacy Interests

In December 2013, Facebook, Google, Yahoo and other tech giants published an open letter calling for "Global Government Surveillance Reform."[101] In addition to the open letter, the companies listed five principles as the bases for their position. Although these companies focused on government surveillance, the first three of their privacy principles equally apply to these companies and other private actors if you substitute "government" with "firms." The fourth principle, unsurprisingly, somewhat subtly seeks to avoid application of these principles to private actors.[102]

Principle one is "Limiting Governments' Authority to Collect Users' Information." The tech giants call for this limitation because of "users'

96. 132 S.Ct. 945, 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

97. Ammori & Pelican, *Media Diversity*, *supra* note 25, at 679–80.

98. *Id.* at 682.

99. *Id.* at 681; Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 981–82 (1996).

100. David Streitfeld, *As New Services Track Habits, the E-Books are Reading You*, N.Y. TIMES, Dec. 25, 2013, at A1.

101. REFORM GOVERNMENT SURVEILLANCE, http://reformgovernmentsurveillance.com/ (last visited Oct. 1, 2014). The full list of companies is: AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo.

102. The fifth principle, "Addressing Conflicts Among Governments," is not applicable to this Article.

reasonable privacy interests" and the notion that the government "should not undertake bulk data collection."[103] This principle equally applies to private companies because it is not the public or private nature of the data processor that matters.[104] Rather, what matters are the reasonable privacy interests of individuals in not being subject to bulk data collection resulting in detailed profiles without their consent.

Principle two calls for "Oversight and Accountability." An opt-in regime is one method for creating oversight and accountability because it would empower individuals to decide whether to opt-in to data processing after receiving information regarding a commercial actor's data practices.[105] Principle three calls for "Transparency About Government Demands" because transparency is "essential to a debate over governments' surveillance powers and the scope of those programs that are administered under those powers."[106] Transparency is also essential to a debate over the data processing activities of online commercial actors. Because firms have a natural incentive to not be transparent in their data processing activities, an opt-in regime nudges them towards transparency, and thus, to oversight and accountability.

The fourth principle, however, seeks to carve out special protections for private actors and to counter the General Data Protection Regulation (GDPR) recently proposed by the European Parliament.[107] If enacted, the European Parliament's proposed GDPR would provide every natural person with the right to object to profiling.[108] The fourth principle of the Big Data actors is titled, "Respecting the Free Flow of Information," and states that "[g]overnments should not inhibit access by companies or individuals to lawfully available information that is stored outside the country."[109] This principle shows that the tech giants do not believe the same principles regarding limits on data collection, oversight, accountability, and transparency equally apply to private actors. The flaw in this principle is that it loses sight of the reasons for these principles in the first place: protecting individual privacy interests from

103. REFORM GOVERNMENT SURVEILLANCE, *supra* note 101.

104. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Cohen, *What Privacy is For*, *supra* note 11, at 3.

105. Other methods that seek to protect privacy also help create oversight and accountability. *E.g.*, MAYER-SCHONBERGER & CUKIER, BIG DATA, *supra* note 9, at 179–82 (proposing a new profession–"algorithmists"–to monitor and advise companies based on their use of algorithms in data processing).

106. REFORM GOVERNMENT SURVEILLANCE, *supra* note 101.

107. The proposed EU Data Protection Regulation would limit a company's ability to share information about EU citizens with companies not subject to EU privacy protections. This Article cites the October 2013 version of the proposed GDPR.

108. EU GDPR, *supra* note 22, at Comp. Art 20(1).

109. REFORM GOVERNMENT SURVEILLANCE, *supra* note 101.

powerful actors, regardless of whether they are public or private.[110]

Vast data collection and surveillance by government actors is of serious concern.[111] The recent and ongoing disclosures of the scope of the government's surveillance programs made possible by leaker Edward Snowden further clarify this point. While government intrusions into online privacy are of serious concern, they are beyond the scope of this Article.[112] There are, however, two points about government surveillance that are relevant here.

First, "the reason government has access to so much data in the first place, in many cases, is because corporations collect it."[113] And, news reports indicate some level of cooperation by private companies in providing the government with data about individuals.[114] Additionally, a recent report recommended limiting the government's expansive surveillance program, in part, because private actors will still possess the data and the government can simply access it upon lawful requests.[115] In other words, even if the government itself no longer collects bulk data, the risk of government surveillance remains high because of the existence of expansive privately possessed data.[116]

Second, this alignment of interests—private actors' commercial interests in data processing for profit and government interest in data processing for purposes of law enforcement—will likely add to the inertia of government regulation that seeks to protect individuals'

---

110. *See also* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012). Ohm proposes reinterpreting the Fourth Amendment to focus on freedom from government power, instead of focusing on privacy. *Id.* at 1311–12. Leaving aside the state action doctrine, individuals should equally be free from excessive power by private actors. At the very least, such power infringes on an individual's autonomy rights and the classification as a private actor does not, or at least should not, make that infringement permissible. *See, e.g.*, Erwin Chemerinksy, *Rethinking State Action*, 80 NW. U.L. REV. 503 (1985).

111. *E.g.*, Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); *but see* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

112. For commentary on government actors and online privacy, see, e.g., Richards, *The Dangers of Surveillance*, *supra* note 104.

113. Kate Kaye, *Prism Could Be a Watershed Moment for Online Privacy Legislation: Or It Could Take the Focus Off Advertising Entirely*, AD AGE (June 10, 2013), http://adage.com/article/privacy-and-regulation/prism-a-watershed-moment-privacy-legislation/242010/?utm_source=mediaworks&utm_medium=newsletter&utm_campaign=adage&ttl=1371493909.

114. Claire Cain Miller, *Tech Companies Concede to Surveillance Program*, N.Y. TIMES, June 8, 2013, at A12. Although tech companies have cooperated with the government to some degree, it appears the government has also covertly collected data from them without their knowledge. Nicole Perlroth & John Markoff, *N.S.A. May Have Hit Internet Companies at a Weak Spot*, N.Y. TIMES, Nov. 26, 2013, at B1 (stating that the N.S.A. appears to have accessed data from Google and Yahoo, among others, by accessing their users' data from Internet backbone providers, such as Level 3, Verizon Communications, BT Group, and Vodaphone).

115. Sanger & Savage, *Obama is Urged to Sharply Curb N.S.A. Data Mining*, *supra* note 87.

116. Neil M. Richards, *Reconciling Data Privacy & the First Amendment*, 52 UCLA L. REV. 1149, 1158–59 (2005).

privacy interests. Despites these obstacles, an opt-in requirement merits consideration because it seeks to protect individual privacy interests and consequently, democracy. One way to help overcome the obstacles presented by industry and government opposition to data privacy reform is to show that an opt-in requirement is supported by, or least consistent with, a law and economics analysis.

B. Privacy and Economic Analysis

Because the financial interest of data processors is a major factor driving the development of Big Data, an economic analysis of the struggle between individuals' privacy rights and firms' financial interests is a common part of the scholarship and the national conversation. An argument often made against increased regulation of data processing is that it will result in increased transaction costs, thereby threatening the information economy and innovation.[117] As one commentator wrote, such an argument should be "taken with a grain of salt."[118] Indeed, basic economic theory, behavioral economics, and an economic theory of privacy each show that one can reasonably make the claim that law and economics theory actually supports the need for regulation.

First, basic economic theory applied to data processing by online commercial actors undercuts arguments against regulation. The basic actor in neoclassical economics is the individual. Further, maximizing individual choice is the *sine qua non* of this theory especially as those individual choices are reflected in market transactions that send reliable price signals. By way of example, "[t]he most common normative justification for a market economy rests on the basic idea that payments signal [individual] preferences."[119] Although individuals often do not pay money for online services or products, some argue that they "pay" with personal information.[120] Data processors then argue that simply by using the Internet, an individual signals a preference or a willingness to allow data processing in exchange for the online goods and services.[121] This rationale is flawed. Individuals are mostly unaware of the uses to which their personal data is put, and thus, cannot consent to what they do not know. Also, online behavioral advertising is not a basic market

117. *E.g.*, Berin Szoka & Adam Theier, *Targeted Online Advertising: What's the Harm and Where We Heading?*, THE PROGRESS AND FREEDOM FOUNDATION, June 2009, at 8; Cohen, *Examined Lives*, *supra* note 6, at 1388.

118. Strandburg, *Free Fall*, *supra* note 24, at 68.

119. *Id.* at 14.

120. *E.g.*, Angwin, *Has Privacy Become a Luxury Good?*, *supra* note 2.

121. Strandburg, *Free Fall*, *supra* note 24, at 15.

involving one seller and one buyer. Advertisers are the actual consumers of data processing, not individuals who have become the product.[122] And, advertisers are not paying customers for their personal data; they are paying the data collectors.

Even if individuals are considered to "pay" for online products and services with their data, that "payment" does not necessarily occur at the point of purchase.[123] Data processing occurs before, during, and after the point of purchase. Data processors can track whether an individual clicked on a particular good, even if they did not buy it and use that data as part of an individual's profile. Some individuals are profiled into categories such as, "Very Elderly," "X-tra Needy," and "Enduring Hardships."[124] Data processors can take previously collected data and connect it with other data, including data purchased from other data processors, for unknown future uses. Post-transaction data processing is a significant source of disutility to an individual precisely because of an individual's lack of knowledge, consent or control of these transactions;[125] and, it is a major issue of contention because some view Big Data's secondary uses as a main source of potential value to be gained from data processing.[126]

In short, there is significant information asymmetry between individuals and online data processors because data processors do not disclose the information they process, they process data at times before and after the point of purchase, and because it is impossible for an individual to signal a preference when data is used post-transaction for a use that is unknown or unavailable at the time of purchase. Thus, the basic economic justification that payment signals preference does not work in the context of online data processing by commercial actors.

Second, from a behavioral economics perspective, opt-in regulation of online data processing by commercial actors can help correct market manipulation.[127] Data processors intentionally create and maintain information asymmetry between themselves and the individual whose data is processed.[128] They provide little opportunity to opt-out of data

---

122. *Id.*

123. *Id.* at 43.

124. STAFF OF S. COMM ON COMMERCE, SCIENCE, AND TRANS., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY, COLLECTION, USE AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES (Dec. 18, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 [*hereinafter* SENATE COMM. REPORT].

125. Strandburg, *Free Fall*, *supra* note 24, at 44. Potential sources of disutility include adverse decisions by potential or existing employers or insurers and price discrimination. *Id.* 45–46.

126. MAYER-SHONBERGER & CUKIER, BIG DATA, *supra* note 9.

127. *See generally* Calo, *Digital Market Manipulation*, *supra* note 2.

128. SENATE COMM. REPORT, *supra* note 124.

processing, let alone opt-in.[129] From a financial perspective, the failure to disclose data processing practices or offer the ability to opt-out (if they provide any option at all) is strategically sound. "Companies have every incentive to keep these transaction costs high in order to discourage consumers from taking steps to avoid data collection."[130] Indeed, "[t]he entire point is to leverage the gap between how a consumer pursuing her self-interest would behave leading up to the transaction and how an actual consumer with predictable flaws behaves when pushed, specifically so as to extract social surplus."[131] Thus, behavioral economics supports an opt-in regime to help reduce market manipulation.

Finally, a law and economics theory of privacy also supports the need for regulation of data processing by online commercial actors. Judge Richard Posner has accurately noted that one purpose of privacy is to conceal harmful, but truthful information about oneself.[132] Under Posner's economic analysis of privacy, this is an invalid or unjustifiable purpose of privacy because it increases transactions costs and risk by creating information asymmetry.[133] Applying this economic theory of privacy to online data processing supports the need for an opt-in requirement. Data processors intentionally seek to prevent individuals from knowing about their data processing practices. Their failure to disclose their data processing practices prior to engaging in data processing increases the risks and transaction costs of individuals whose data is processed without notice or consent.

In conclusion, some economics analysis supports an opt-in requirement. Payment does not signal preference in the online data processing context because the actual consumer is the advertiser purchasing the data, not the individual whose data is processed. And, the individual lacks the necessary information about data processing to make an informed decision whether to "pay" with her data. Further, a behavioral economics view strongly suggests that there is a market failure when it comes to individual online privacy because data processors are intentionally creating and maintaining informational asymmetries.[134] Finally, under Judge Posner's law and economics view of privacy, online data processors should not be entitled to maintain this information asymmetry because it is created to hide the data processing

129. *Id.*

130. Strandburg, *Free Fall*, *supra* note 24, at 61; Sovern, *Opting-In, Opting-Out*, *supra* note 44.

131. Calo, *Digital Market Manipulation*, *supra* note 2, at 1023.

132. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399 (1978).

133. *Id.* at 398.

134. *See generally* Strandburg, *Free Fall*, *supra* note 24; Calo, *Digital Market Manipulation*, *supra* note 2.

activities from the individuals whose data is processed. Regulation is necessary to correct the market failure because data processors have every incentive to maintain the information asymmetry. At the very least, these indicia of market failure cast serious doubts on claims that self-regulatory solutions are sufficient.

IV. OPTING-IN

The concept of an opt-in requirement as a method to protect informational privacy is not new.[135] This Article seeks to provide unique contributions to prior online privacy literature through its First Amendment analysis in Part V, and in this Part, through a summary of opt-in analysis by government actors, including the Federal Trade Commission (FTC), the White House, courts, and the European Union (EU).

A. Opting-Out Is Ineffective

An opt-out regime is insufficient to protect individuals' privacy interests from the actions of online commercial data processors for several reasons. First, individuals often fail to exercise their right to opt-out in the online data processing context, as well as other contexts.[136] For many years, data processing industry actors have known that individuals often fail to exercise their right to opt out. When Netscape's Navigator 4.0 was released in 1997, it included an option for individuals to opt-out of all cookies or certain types of cookies.[137] A draft proposal by the Internet Engineering Task Force would have required individuals

---

135. *E.g.*, Location Privacy Protection Act of 2012, S. 1223, §3, 112th Congr. (2012) (the act would have required private actors to receive an individual's "express authorization" before collecting or sharing geolocation data from automobile, mobile phones, and other devices); Sovern, *Opting-In Opting-Out*, *supra* note 44; Rick Bruner, *Interactive: 'Cookie' Proposal Could Hinder Online Advertising: Privacy Backers Push for More Data Controls*, ADVERTISING AGE, Mar. 31, 1997, (http://adage.com/article/news/interactive-cookie-proposal-hinder-online-advertising-privacy-backers-push-data-controls/73718/.

136. The Driver's Privacy Protection Act of 1994 (DPPA) provides an example of a law changing from an opt-out to an opt-in approach in order to be more effective in protecting privacy. 18 U.S.C. § 2721. Under the original DPPA, states were not permitted to release a driver's personal information without consent, but consent was presumed unless the driver opted-out. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322 § 300002, 108 Stat, 2099 (1994). In 1999, Congress amended the DPPA by requiring a state to receive a driver's express consent before it could release the driver's information. Department of Transportation and Related Agencies Appropriation Act of 2000, Pub. L. No. 106-69, § 350(c)-(e), 113 Stat. 986, 1025 (1999).

137. Rick E. Burner, *Advertisers Win One in Debate Over Cookies*, ADVERTISING AGE, May 12, 1997, http://adage.com/article/news/advertisers-win-debate-cookies/405/, http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html?pagewanted=all.

to opt-in before third-party cookies were accepted. One industry member described the opt-in proposal as "terrible" from the perspective of advertising companies.[138]

Although advertisers were thankful that the Navigator did not adopt the opt-in proposal, they still had concerns about the opt-out option. Advertising Age informed readers not to worry about this change precisely because of the ineffectiveness of an opt-out default: "because the vast majority of Web users never bother to change their cookie preferences, the effect on companies that use cookies as targeting tools will be minimal."[139] Online data processors have a natural preference for an opt-out design as opposed to opt-in because it is essentially "nudging for profit."[140]

Second, individuals often fail to opt-out because of the lack of information they have regarding data processing. This information asymmetry is intentionally perpetuated by the data processing industry. Terms in a privacy policy concerning data processing are commonly broad, vague, and buried. Third, not only are terms of data processing intentionally broad, vague, and buried, the data processing tools themselves are intentionally hidden. The design of cookies, web bugs, beacons, and other tracking technologies are intentionally designed to avoid detection and control by individual users.[141]

Finally, even if an opt-out option is offered to individuals, the scope of the opt-out may be rather limited and difficult to exercise. The Network Advertising Initiative (NAI) allows individuals to opt-out of being served behavioral advertising, but does not allow individuals to opt-out of data collection or profiling.[142] This limited ability to opt-out is insufficient because it does not prevent data processors from continuing to place tracking technologies on individuals' devices or

---

138. *Id.*

139. *Id.* Negative option marketing is an example of similar market manipulation. Calo, *Digital Market Manipulation*, *supra* note 2, at 1002.

140. Calo, *Digital Market Manipulation*, *supra* note 2, at 1001.

141. For a summary of some of the these types of tracking technologies, *see e.g.*, Christine Suzane Davik, *We Know Who You Are and What You're Made Of: The Illusion of Internet Anonymity and Its Impact on Protection From Genetic Discrimination*, 64 CASE WESTERN L. REV. 17, 23–27 (2013).

142. TUROW, DAILY YOU, *supra* note 4, at 181. Since the publication of Turow's book, the Digital Advertising Alliance (DAA) has addressed this issue to some degree:

> More recently, the DAA addressed one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the consumer opt out extends beyond simply blocking targeted ads to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.

FTC, RAPID CHANGE, *supra* note 21, at 54 (*citing* Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf).

from creating profiles of individuals. The NAI's limited opt-out mechanism has also been criticized for being "cumbersome and inaccessible."[143]

Although there has been some progress,[144] not much has changed since 1997 when Advertising Age trumpeted the defeat of an opt-in feature that would have required a user to opt-in before Navigator would allow third-party cookies to be accepted by an individual's computer. In December 2013, a Senate Committee Report concluded that individuals "should expect that data brokers will draw on this data without their permission to construct detailed profiles on them reflecting judgments about their characteristics and predicted behaviors."[145] From a descriptive perspective, the Senate Committee Report's conclusion is accurate. From a normative perspective, however, individuals have legitimate interests (if not established rights) in not being tracked and profiled without consent. Both the EU Charter on Fundamental Human Rights[146] and Supreme Court dicta in *Sorrell v. IMS Health* provide support for this normative perspective.[147] Because an opt-out regime is ineffective, an opt-in regime is necessary to protect these legitimate privacy interests.

B. Opt-In Law and Policy in the Data Privacy Context

Although there is currently no law that generally requires online commercial actors to receive an individual's opt-in consent prior to data processing, there has been some action and policy recommendations by government actors on this issue. This subpart provides some examples of government recommendations and actions, as well as case law regarding an opt-in requirement in the data privacy context. The subpart concludes with a summary of the opt-in requirement of the EU's recently proposed General Data Protection Regulation.

---

143. FTC, SELF-REGULATORY PRINCIPLES, *supra* note 28, at 10.

144. In July 2013, the Digital Advertising Alliance announced new self-regulatory rules requiring that "ad networks, app developers and others must obtain people's opt-in consent before collecting geolocation information and address-book data." Wendy Davis, *DAA Mobile Privacy Rules Require Opt-In Consent for Address Books, Geolocation*, MEDIAPOST, July 24, 2013, http://www.mediapost.com/publications/article/205161/daa-mobile-privacy-rules-require-opt-in-consent-fo.html. But, the new rules won't go into effect for at least nine months and the enforcement mechanism is uncertain. *Id.*

145. SENATE COMM. REPORT, *supra* note 124, at 35.

146. "Everyone has the right to the protection of personal data concerning him or her." Charter of Fundamental Rights of the European Union, 2 Art. 8(1), 012/C 326/02.

147. 131 S. Ct. 2653 (2011), *supra* note 1.

1. Federal Trade Commission Opt-In Recommendations & Actions

The FTC has held numerous workshops, issued several reports, and taken official action regarding online privacy.[148] These reports focus on data collection practices, industry self-regulation, and recent technological advances that affect consumers' privacy. Some of these FTC recommendations and actions relate to an opt-in or similar requirement.

In 1998, the FTC provided a report to Congress advising that Fair Information Practice Principles (FIPPs) should be followed when collecting personal information.[149] Of the five principles, the two most relevant to this Article are the principles of Notice/Awareness and Choice/Consent.[150] The FTC report describes the Notice/Awareness principle as the "most fundamental" because without notice to data processing practices, a "consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[151] The 1998 Report included analysis of industry guidelines and noted that none of the guidelines at the time adopted an opt-in regime for adults.[152] The Report concluded that as of 1998, the Commission had not seen evidence of effective self-regulation, including a failure to provide sufficient notice of data processing practices, let alone offer an opt-in design.[153] Although the Report recommended that Congress pass legislation to protect children twelve and under from data processing, including two opt-in requirements, it made no recommendation regarding data processing of adults.[154]

148. For a convenient list of these activities from 1970–2012, *see* FTC, RAPID CHANGE, *supra* note 21, at Appendix A (a color coded index of "FTC Privacy Milestones," including laws and rules, cases, reports, workshops, and education).

149. FIPPs were first set forth in, UNITED STATES DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973). Since that time, these principles have been developed by a variety of government agencies. FEDERAL TRADE COMMISSION, ONLINE PRIVACY: A REPORT TO CONGRESS 48, n. 27 (1998) (collecting documents) [*hereinafter* FTC REPORT TO CONGRESS].

150. The other three principles are: (1) Access/Participation; (2) Integrity/Security; and (3) Enforcement/Redress. FTC REPORT TO CONGRESS, *supra* note 149, at 7. These principles are also relevant to online privacy. If an individual does not have Access/Awareness to an online commercial actor's profile of her, she cannot make a determination if the information is accurate. Without laws requiring data processors to maintain the Integrity/Security of data collected, individuals are at risk of further privacy erosion. Without a right to Enforcement/Redress, there is little deterrent to commercial data processing.

151. FTC, REPORT TO CONGRESS, *supra* note 149, at 7.

152. FTC, REPORT TO CONGRESS, *supra* note 149, at 16. Some industry guidelines included an opt-in requirement in the context of children. Id. at 17.

153. FTC, REPORT TO CONGRESS, *supra* note 149, at 41.

154. The opt-in requirements for children 12 and under were: (1) receiving a parent's opt-in consent prior to collecting information that could be used to contact the child offline, and (2) receiving a parent's opt-in consent prior collecting personal identifying information that would be disclosed to the

In 2009, the FTC published a staff report regarding data collection and behavioral advertising that included discussion of an opt-in mechanism as a possible requirement.[155] The report noted that consumer and privacy advocates desired an opt-in requirement prior to data collection.[156] Ultimately, however, the report did not recommend that an opt-in mechanism should be generally required.[157] Rather, it limited its opt-in recommendation to "uses of data that raise heightened privacy concerns—specifically, material changes affecting the use of previously collected data and the use of sensitive consumer data."[158]

Examples of sensitive data included health, finance, or sexual preference data.[159] The FTC staff report further encouraged advertisers "to consider whether there may be certain categories of data that are so sensitive that they should never be used for behavioral advertising."[160] For other uses of data, the FTC staff report simply recommended that consumers have a "clear, easy-to-use, and accessible" choice regarding data processing, regardless of whether that choice is an opt-in or an opt-out mechanism.[161] This 2009 FTC staff report has been criticized as reflecting too much influence by data processors, in part, because it recommended that other than "sensitive data," data processing could occur on an opt-out basis.[162]

In 2012, the FTC issued its report, *Protecting Consumer Privacy in*

---

public or third-parties. FTC, REPORT TO CONGRESS, *supra* note 149, at 43. Even in the context of children ages 12 and under, the Report recommended opt-out mechanisms for other types of data processing. Id. Subsequent to this Report, Congress passed the Children's Online Privacy Protection Act of 1998. 15 U.S.C. §§ 6501–6506. Although it does not use the term "opt-in," it does require online actors to receive "verifiable parental consent" when engaging in data processing that involves personal information from children ages 12 and under. 15 U.S.C. § 6502(b)(ii). "Verifiable parental consent" is not required under all circumstances. 15 U.S.C. § 6502(b)(2). Moreover, the definition of "verifiable parental consent" seems to leave room for something less than the express, affirmative, and informed opt-in requirement proposed here:

> The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

15 U.S.C. § 6502(b)(ii).

155. FTC, SELF-REGULATORY PRINCIPLES, *supra* note 28, at 16, 32.

156. *Id.* at 32.

157. *Id.* at 32, n. 63.

158. *Id.*

159. TUROW, DAILY YOU, *supra* note 4, at 174.

160. *Id.*

161. FTC, SELF-REGULATORY PRINCIPLES, *supra* note 28, at 32, n. 63.

162. TUROW, DAILY YOU, *supra* note 4, at 174–75.

an Era of Rapid Change.[163] The report includes discussion about the use of an opt-in requirement in the context of deep packet inspections (DPI).[164] Some commenters advocated for an opt-in requirement before DPI could occur because of the vast amount of information provided via DPI.[165] Internet Service Providers (ISPs) objected stating that they do not use DPI for marketing purposes, that similar amounts and types of data can be gathered via other tracking technologies, and that the FTC's principles on data processing should apply consistently, regardless of the particular technology used.[166] While the FTC stated that DPI is more invasive than cookies, it agreed that its proposal should be technology neutral.[167] The opt-in proposal here is consistent with the ISPs call for similar treatment of data processors because it applies to all types of data processing by commercial actors, regardless of technology used.

Although the 2012 Report did not recommend receiving opt-in consent for all data processing, it did acknowledge that data may be sensitive depending on the person involved.[168] Consistent with its 2009 staff report, the 2012 report maintains its recommendation for an opt-in requirement when a company makes a material change to its privacy representations or when it collects sensitive data.[169] At least one type of change that is "material" is sharing information with third-parties when a prior privacy representation stated that data would not be shared with third-parties.[170] As far as what data is labeled "sensitive," the FTC noted general consensus on data regarding children, health, financial,

---

163. FTC, RAPID CHANGE, *supra* note 21.

164. Deep Packet Inspection (DPI) presents both costs and benefits to individuals:

> Deep packet inspection helps your ISP block the spread of computer viruses, identify illegal downloads, and prioritize the data transmitted by bandwidth-heavy applications like video chat and VoIP applications to alleviate network congestion and improve your service. Law enforcement officials (with a court order) can use these tools to lawfully intercept communications of suspected criminals.
>
> But deep packet inspection has a dark side, and in the absence of strict legal restrictions, your ISP is free to root through all the information you exchange online and use it as they see fit. Personal data like your age, location, and shopping records can be logged and sold in anonymized batches to advertising companies, and law enforcement agents can monitor and curtail your Internet access without your knowledge. Without strict limitations to preserve user privacy, this sort of deep data filtering can significantly impair your ability to remain anonymous online.

Alex Wawro, *What Is Deep Packet Inspection*, PCWORLD.COM, Feb. 1, 2012, http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html.

165. FTC, RAPID CHANGE, *supra* note 21, at 55.

166. *Id.* at 55–56.

167. FTC, RAPID CHANGE, *supra* note 21, at 56.

168. *Id.*

169. *Id.* at 57.

170. FTC, RAPID CHANGE, *supra* note 21, at 58.

Social Security numbers and precise geolocation data.[171]

In addition to holding workshops and issuing reports and recommendations, the FTC has engaged in some official action involving opt-in requirements. In 2004, the FTC issued an Order requiring Gateway Learning Corporation to receive an individual's "express affirmative ('opt-in') consent" prior to sharing data with third-parties.[172] This order, however, is limited in several respects. The order applied only to Gateway Learning Corporation. It applied only to "personal information," which as discussed above is likely a futile limitation in light of the ability to re-identify individuals in the Big Data era.[173] Finally, the impetus for the order was that Gateway Learning Corporation violated its own privacy policy. Gateway had a privacy policy that promised not to sell personal information to third-parties. Subsequently, it changed that policy, allowing the disclosure of personal information to third-parties. The order only required Gateway to receive opt-in consent for the disclosure to third-parties from individuals that made an agreement under the old policy.[174] Opt-in consent was not required for anyone that entered into an agreement under the new policy; their personal information could be disclosed to third-parties.

In 2011, the FTC took official action against Google and Facebook in separate investigations because of concerns about the privacy of their users.[175] Both of these orders required the companies to create a comprehensive privacy program to protect individual users' identifiable information.[176] These orders specifically require that each company obtain an individual's "affirmative, express consent" prior to sharing non-public information that materially exceeds the individual's privacy settings, and disclose the categories of information shared and the "identity or specific categories of such third parties" with whom it's shared.[177]

Thus, a theme emerges from the FTC reports and orders in the online

---

171. FTC, RAPID CHANGE, *supra* note 21, at 59.

172. Gateway Learning Corp., FTC Docket No. C-4120 (Sept. 10, 2004), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917do0423047.pdf.

173. *See* Part II.A, above.

174. Gateway Learning Corp., FTC Docket No. C-4120, at 3.

175. Google Inc., FTC Docket No. C-4336 (Oct. 13, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzorder.pdf; Facebook, Inc., FTC File No. 092-3184 (Nov. 29, 2011), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf. For a summary of FTC enforcement actions, *see* Fatima Nadine Khan, *Survey Of Recent FTC Privacy Enforcement Actions and Developments*, 68 BUS. LAW. 225 (2012).

176. Google Inc., F.T.C. File No. 092-3136 at 4–5; Facebook Inc., F.T.C. File No. 092-3184 at 5–6.

177. Google Inc., Id. at 4; Facebook Inc., Id. at 4. These orders also require company-wide privacy programs that outside auditors will assess for the next twenty years. Google Inc., Id. at 5; Facebook Inc., Id. at 6.

privacy context. Opt-in recommendations are generally limited to material changes in a preexisting privacy policy and "sensitive" data. But, just as anonymity cannot be relied upon to protect privacy by segregating personally identifiable information from non-personally identifiable information, neither can privacy be protected by segregating sensitive from non-sensitive information. The interconnectedness of data and data processors can quickly turn non-sensitive data into "sensitive" data. FTC action to date on opt-in recommendations and actions is moving in the right direction, but is not comprehensive enough.

2. White House Action

In 2012, the White House issued its report, *Consumer Data Privacy in a Networked World.*[178] The report acknowledged that use of personal data by commercial actors does raise privacy concerns and therefore, individuals should have some control.[179] Although the term "opt-in," does not appear in the report,[180] the first item in the Consumer Privacy Bill of Rights is: "Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it."[181] This discussion includes the principle that consumers should be afforded "appropriate control" and that companies "should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure."[182] Further, this principle requires that companies "should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place."[183] Thus, while not expressly recommending an opt-in requirement, such a requirement would be consistent with the Consumer Privacy Bill of Rights.

In 2014, the Editorial Board of the *New York Times* criticized the Obama Administration and Congress for the failure to act on the 2012 Consumer Privacy report.[184] After noting that a new White House consumer privacy report is expected in late April or early May 2014,[185]

178. WHITE HOUSE PRIVACY REPORT, *supra* note 93.

179. *Id.* at 12.

180. The report notes that industry actors did create some self-regulatory opt-outs from targeted advertising. *Id.* at 11–12.

181. *Id.* at App. A, at 47.

182. *Id.* at 11.

183. Id.

184. Editorial Board, *A Second Front in the Privacy Wars*, N.Y. TIMES Feb., 23, 2014 http://www.nytimes.com/2014/02/24/opinion/a-second-front-in-the-privacy-wars.html#.

185. John Podesta, *Big Data and the Future of Privacy*, www.whitehouse.gov, Jan. 23, 2014,

the *Times* called for this report to provide "specific legislative proposals to give consumers more control of [their] information."[186] The White House issued its report on May 1, 2014 with policy recommendations, including some specific legislative proposals.[187] Of particular relevance to this Article, the White House report questions whether a notice and consent based approach is the best method to protect privacy in the Big Data era.[188]

Instead of focusing on collection, the report recommends that focusing on "how data is used and reused would be a more productive basis for managing privacy rights in a big data environment."[189] The report focuses on use rather than collection because the authors do not want to impede the use of Big Data for publicly beneficial purposes. But, it also recognizes that "consumers still have a valid interest in 'Do Not Track' tools that help them control when and how their data is collected."[190] Thus, the report is somewhat equivocal on the role of consent.

There are at least two reasons why an opt-in requirement in the commercial data processing context is an important part of the solution. First, once data is collected, "it may prove impossible to make our data disappear completely."[191] Second, data collected by commercial data processors is generally not used for publicly beneficial purposes; it is used for private financial benefits.[192] Thus, while focusing on use and

---

http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

186. Editorial Board, *A Second Front in the Privacy Wars*, N.Y. TIMES Feb., 23, 2014 http://www.nytimes.com/2014/02/24/opinion/a-second-front-in-the-privacy-wars.html#.

187. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 58–68. This report focuses on legal, ethical, and social norms that require consideration in light of big data developments. A parallel White House privacy report was also issued on May 1, 2014. *See* PRESIDENT'S COUNCIL OF ADVISORS FOR SCIENCE & TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (May 1, 2014).

188. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 61 ("While notice and consent remains fundamental in many contexts, it is now necessary to examine whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment."). For the reasons articulated here, receiving an individual's opt-in consent, at least prior to processing by commercial actors, is an important mechanism because it helps restore some balance between individuals and commercial actors by empowering individuals prior to data collection.

189. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 61.

190. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 16, at 62.

191. Shaun Spencer, *The Surviellance Society and the Third-Party Privacy Problem*, 65 S. CAR. L. REV. 373, 400 (2013).

192. *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 761–62 (1985) (credit report is not a matter of public concern, it is "speech solely in the individual interest of the speaker and its specific business audience"); *and* Trans Union Corp. v. F.T.C., 245 F.3d 809, 818 (D.C. Cir. 2001) (Like the credit report in *Dun & Bradstreet*, "the information about individual consumers and their credit performance communicated by Trans Union target marketing lists is solely of interest to the company and its business customers and related to no matter of public concern.").

reuse of collected data is a wise recommendation, the White House report fails to sufficiently focus on preventing the collection of data without consent and that failure is detrimental to individuals' privacy.

3. Opt-In Analysis in Data Privacy Cases

There is little case law on an opt-in requirement in the context of online commercial data processors and the case law that exists does not support requiring an opt-in mechanism before data processing. In *U.S. West, Inc. v. FCC*,[193] the Tenth Circuit analyzed an opt-in requirement under the commercial speech doctrine and held that it violated the First Amendment rights of the commercial actor. The FCC issued an order requiring telecommunications services to receive a customer's opt-in consent prior to using Customer Proprietary Information (CPNI) for marketing purposes. CPNI includes sensitive information, "such as to whom, where, and when a customer places calls."[194] The FCC considered an opt-out approach, but chose an opt-in approach because of privacy concerns of customers.

Although the court was skeptical that customer privacy in this context was a substantial state interest, it accepted it as such for purposes of its analysis.[195] The court, however, held that the FCC failed to establish that the opt-in requirement directly and materially advanced the asserted privacy interest[196] and that it failed to "adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy."[197] The dissent disagreed noting that opt-outs are not as effective as opt-ins when the goal is informed consent because opt-outs result in higher risks of uninformed approval based on a failure to take action to opt-out.[198]

In *Sorrell v. IMS Health,* the Supreme Court considered an opt-in requirement in the context of physicians' prescribing data.[199] A Vermont law prohibited the sale, use, or disclosure of a physician's prescribing data to pharmaceutical companies or their "detailers,"[200]

---

193. 182 F.3d 1224 (10th Cir. 1999).

194. *Id.* at 1235.

195. *Id.* at 1236–37. The other asserted state interest was that an opt-in requirement promoted competition, but that interest is not relevant here.

196. *Id.* at 182 F.3d at 1236.

197. *Id.* at 1238–39.

198. *Id.* at 1247 (Briscoe, J. dissenting).

199. Sorrell v. IMS Health, 131 S. Ct. 2653. *Sorrell* is discussed in more detail in Part V.B and C, below.

200. Pharmaceutical companies uses "detailers" to help increase sales of drugs. Detailers visit physicians and bring drug samples and medical studies to persuade the doctor to prescribe particular drugs. When a detailer knows a physician's prescribing history, it allows for a more effective pitch. *Id.* at 2659–60. Because detailing is an expensive undertaking, "pharmaceutical companies most often use it to promote high-profit brand-name drugs protected by patent." *Id.*

unless the prescribing physician consented. In part, Vermont justified this law as means to "protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship."[201] But, this law allowed the same information to be used and disclosed to others, such as researchers, without requiring the prescribing physician's consent. Because the Vermont law disfavored pharmaceutical companies and was limited in its ability to protect the asserted privacy interests, the Court held that the statute violated their First Amendment rights. Thus, the opt-in consent requirement did not save the statute. In a subsequent case, *Knox v. SEIU*,[202] the Court expressly required an opt-in approach as a matter of First Amendment law. Because that case does not involve data privacy it is not addressed here, but it is discussed in Part V. E, below.

4. The European Union's Proposed Opt-In Regime

The European Parliament recently proposed a General Data Protection Regulation (GDPR). This proposed regulation is extensive, including over 3000 proposed amendments. In addition to the extensive length and scope of the regulation, the proposal is highly contentious, including lobbying activity by U.S. data processing companies. This Article focuses on the opt-in requirement of the proposed regulation, which serves as the model for the type of opt-in requirement proposed here.

The GDPR defines an individual's "consent" to data processing as "any freely given, specific, informed and explicit indication . . . either by a statement or by a clear affirmative action."[203] The Regulation has five conditions for consent. First, the data processor bears the burden of proving that the individual provided consent.[204] Second, consent to data processing must be clearly "distinguishable in its appearance" from consent to other matters.[205] This requirement seeks to avoid the problem of hiding terms regarding data processing among other contractual terms. Third, the individual must be provided with the right to withdraw consent at any time.[206] This right does not allow the individual to retroactively revoke consent from previously consented-to data

201. *Id.* at 2667. Improving public health and reducing healthcare costs were the state interests that Vermont asserted in support of the law. *Id.*

202. 132 S. Ct. 2277 (2012).

203. EU GDRP, *supra* note 22, at Comp. Art. 4(8).

204. EU GDPR, *supra* note 22, at Comp. Art. 7(1).

205. EU GDPR, *supra* note 22, at Comp. Art. 7(2).

206. EU GDPR, *supra* note 22, at Comp. Art. 7(3).

processing.[207] Fourth, "[c]onsent shall be purpose limited" and automatically loses validity once the purpose is fulfilled or the use of the data is no longer necessary for that purpose.[208] Finally, "execution of a contract or the provision of service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or provision of the service."[209]

Although the GDPR does not explicitly use the term "opt-in," its definition of consent coupled with the conditions for valid consent show that it does require opt-in consent before data processing may occur. One of the recitals makes this point even clearer: "The use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent."[210] In other words, an opt-out approach is not sufficient.

One commentator has noted that the United States and the European Union are headed on "collision" course regarding privacy regulation.[211] Although the emphasis on conflict between EU and U.S. privacy law represents the majority view, some commentators have argued that there is more harmony between the U.S. and the EU's respective privacy law regimes than is commonly acknowledged and that there is hope for more harmony.[212] While the EU's proposed GDPR generally supports the view that EU and U.S. privacy law and policy are in conflict, there are some signs of overlap, at least in the context of an opt-in requirement.

The FTC's 2012 Rapid Change report included some incremental steps towards an opt-in regime, similar to that proposed by the EU. One condition for consent under the EU's General Data Protection Regulation is that the consent to data processing must be "clearly distinguishable" from consent to other terms.[213] The FTC provided an example that is consistent with this EU condition.

Companies may seek "affirmative express consent" from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described. Thus, for example, requiring the consumer to scroll through a ten-page disclosure and click on an "I accept" button would not constitute affirmative express

207. Id.

208. EU GDPR, *supra* note 22, at Comp. Art. 7(4).

209. Id.

210. EU GDPR, *supra* note 22, at Comp. Art. 7, Recital 33.

211. Paul M. Schwartz, Symposium: Privacy and Technology: *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

212. *See generally*, Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365 (2013); *and* Peter Swire, *Peter Hustinx and Three Clichés about E.U.-U.S. Data Privacy*, DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? CONTRIBUTIONS IN HONOUR OF PETER HUSTINX, EUROPEAN DATA PROTECTION SUPERVISOR (2004–2014).

213. EU GDPR, *supra* note 22, at Comp. Art. 16(2).

consent.[214]

Another condition for consent under the EU's GDPR is that consent to the transaction for the primary product or service cannot be conditioned on consent to data processing that is unnecessary for the underlying transaction.[215] The FTC made a similar recommendation, at least for important services where individuals have few alternatives. The FTC offered the provision of broadband services as one example of an important service where individuals have few alternatives and recommended that the provision of broadband services not be conditioned on allowing the broadband service provider to track all of the individual's online activity for marketing purposes.[216] The FTC, however, expressly limited its recommendation to "markets for important services where consumers have few options."[217] The report does not give examples of markets for "less important products or services" where requiring consent to data processing may be tied to the underlying transaction on a take it or leave it basis. A 2013 FTC report, however, may shed some light on such an example.

The FTC's report, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising*, discusses the use of negative option marketing, such as automatic enrollment in a cooking club with purchase of a Dutch oven.[218] Rather than recommend that negative option marketing generally be replaced with an opt-in mechanism, the report recommends improvements in disclosures of negative options. One such improvement is that the individual must make an express affirmative action, such as clicking a box to indicate assent, to be subject to the negative option marketing. On first impression, this seems to be a convoluted way of recommending an opt-in regime. The problem, however, is the example in the report does not allow an individual to purchase a Dutch oven without also accepting enrollment in the cooking club. Perhaps this tie-in requirement is not particularly troubling in the context of purchasing a Dutch oven. In the context of online privacy, however, requiring consent to secondary data processing in order to receive the primary service or good is troubling. As discussed above, the EU's proposed GDPR would prohibit such tie-ins.

In conclusion, an opt-in requirement prior to data processing by online commercial actors is a necessary nudge because these firms have

214. FTC, RAPID CHANGE, *supra* note 21, at 57, n.274.

215. EU GDPR, *supra* note 22, at Comp. Art. 7(4).

216. FTC, RAPID CHANGE, *supra* note 21, at 51–52.

217. Id. at 51.

218. FTC, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING (March 2013), A-23-24, (2013), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf (*hereinafter*, FTC, .COM DISCLOSURES).

the natural financial incentive to continue engaging in intentionally opaque data processing practices, practices that conflict with individual privacy interests. Thus, before online commercial actors process data, they must receive an individual's express, affirmative, and informed consent. The EU's proposed GDPR provides a sound model for this type of opt-in regime. In addition to the GDPR, Fair Information Practice Principles dating back to 1973 include Choice/Consent as a foundational principle and the FTC has issued several reports invoking these principles. If Congress passes legislation that requires online commercial data processors to receive an individual's affirmative, express, and informed opt-in consent prior to data processing, First Amendment challenges will surely follow. The next Part provides an analysis of the constitutional permissibility of such an opt-in requirement.

V. FIRST AMENDMENT ANALYSIS OF AN OPT-IN REQUIREMENT

In *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, the Court set forth the test for determining whether a regulation of commercial speech violates the First Amendment.[219] The position of this Article is two-fold. First, an opt-in requirement prior to data processing is constitutionally permissible under a faithful application of the *Central Hudson* test, but the Court has eroded the doctrine making it harder for a regulation of commercial speech to withstand First Amendment scrutiny. Second, even if the Court would not uphold an opt-in requirement pursuant to the commercial speech doctrine, there is another possible argument supporting the constitutionality of an opt-in requirement. After analyzing the commercial speech doctrine, I draw an analogy to *Knox v. SEIU, Local 1000*.[220] In *Knox*, the Court held that an opt-in mechanism was constitutionally required by the First Amendment in the context of extracting fees from non-members of public sector unions. Before providing further analysis on these two issues, however, a debate about the intersection of data processing and the First Amendment must be noted.

A. Data Is Speech, At Least Sometimes

There is a debate whether data is speech subject to First Amendment scrutiny.[221] This debate remains unresolved in the courts because it has

219. 447 U.S. 557 (1980).

220. 132 S. Ct. 2277 (2012).

221. *Compare, e.g.*, Neil M. Richards, *Reconciling Data Privacy & the First Amendment*, 52

not been fully litigated, even in cases where it seems that the question is a threshold issue.[222] Part of the debate involves distinguishing information gathering from information.

Neil Richards has argued that information gathering is not subject to First Amendment scrutiny because it is conduct, not speech.[223] Richards and others note that several laws involving speech do not raise First Amendment scrutiny, such as certain criminal, securities, intellectual property, sexual harassment, and labor laws.[224] The Court similarly observed that "it has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed."[225] Like other laws that involve a speech component, data processing is arguably conduct that is not subject to First Amendment scrutiny. The view of data processing as conduct not subject to the First Amendment, however, is not universal.

Jane Bambauer has argued that data collection is speech subject to First Amendment analysis because the reasoning in cases that draw a distinction between information and information gathering is flawed.[226]

UCLA L. REV. 1149 (2005), *with* Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV.57 (2014). Others argue that focusing on the policy choices regarding data privacy is more productive than debating the proper categorization of data for First Amendment purposes. *See* Solove, *Virtues of Knowing Less*, *supra* note 44, at 981; Cohen, *Examined Lives*, *supra* note 6, at 1419–22. Neither Solove nor Cohen reject the notion that First Amendment concerns are implicated by data privacy regulation.

222. Referring to *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) and *United Reporting Publ'g Corp. v. Los Angeles Police Dept.*, 146 F.3d 1133 (9th Cir. 1998), *rev'd sub nom. Los Angeles Police Dept. v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999), Cohen expressed surprise that "neither court (and, for that matter, none of the parties) question the presence of 'communication' at the collection, processing, and exchange stages—a threshold requirement either for *Central Hudson* scrutiny or for the stricter scrutiny that a narrowed conception of commercial speech might require." *See* Cohen, *Examined Lives*, note 6, at 1413–14. Additionally, the *Sorrell* Court did not engage in any analysis whether a physician's prescribing history data was speech.

223. Richards, *Reconciling Data Privacy & the First Amendment*, *supra* note 221, at 1182–90; *see also* Jedediah Purdy, *The Roberts Court v. America: How the Roberts Supreme Court is using the First Amendment to craft a radical, free-market jurisprudence*, DEMOCRACY, Issue No. 23, 51 (Winter 2012) ("The stranger and more innovative aspect of *Sorrell [v. IMS Health]* is that the case extended First Amendment protection beyond anything recognizable as speech. . . . [M]ost of what the Vermont decision protects is not verbal expression or even political spending but simply the sale of data."), *available at*: http://www.democracyjournal.org/pdf/23/the_roberts_court_v_america.pdf .

224. Richards, *Reconciling Data Privacy & the First Amendment*, *supra* note 221, at 1171 (*citing* Kent Greenwalt, SPEECH, CRIME, AND THE USES OF LANGUAGE 40, at 58, 79–140 (1989); Kent Greenwalt, *Criminal Coercion and Freedom of Speech*, 78 NW. U. L. REV. 1081 (1983); Kent Greenwalt, *Speech and Crime*, 1980 AM. B. FOUND. RES. J. 645; Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1777–84 (2004)).

225. Ohralik v. Ohio State Bar Association, 436 U.S. 447, 456 (1978) (*quoting* Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949)).

226. Bambauer, *Is Data Speech?*, *supra* note 221, at 61. *Cf.*, Ashutosh Bhagwat, *Producing Speech*, 56 WM. & MARY L. REV. (forthcoming 2015) (Bhagwat contends that not only speech itself

Bambauer supports her position, in part, by relying on a right to receive information discussed in *Virginia Pharmacy*.[227] I highlight reliance on the right to receive information because a commercial data processor could argue that such a right precludes an opt-in requirement prior to data processing. As discussed below, however, the commercial speech doctrine is primarily focused on the interests of the individual listener, not the commercial speaker.[228] The right to receive information may be a proxy for protecting individual and societal interests such that a commercial speaker and individual listener may not have equivalent rights to receive information in the commercial speech context.[229]

In any case, asking whether data is speech is too broad of a question,[230] just as asking whether a blogger is a journalist for the purpose of shield law protection is too broad of a question. Sometimes a blogger should be afforded the protections of a shield law, despite not satisfying the traditional notion of who qualifies as a "journalist."[231] Sometimes data is speech. More specifically, at least some aspects of data processing involve speech subject to First Amendment scrutiny because of the importance of the expressive value of the speech at issue, while others do not.

If I send an email using Gmail, Google uses the content of my email to target advertising at me and create a profile about me. Speech is unquestionably involved (i.e. the words I typed into my email) and has now been transformed into data "collected" by Google. The issue in this instance does not seem to be whether data is speech because my email has expressive value. Rather, it seems to be a question of whether Google has the right to use the content of my email for purposes other than transmitting the email to the intended recipient. Collecting my geolocation data, however, seems to be conduct that might not qualify as speech subject to First Amendment scrutiny because it "is not collected, used or sold for its expressive content at all; it is a tool for processing

---

receives First Amendment protection, but also that conduct required to produce speech receives at least some First Amendment protection).

227. Bambauer, *Is Data Speech?*, *supra* note 221, at 74–75.

228. See Part V.B.2, below.

229. See Part, V.B.4, below.

230. *See*, Agatha Cole, Note, *Internet Advertising After Sorrell v. IMS Health: A Discussion on Data Privacy & the First Amendment*, 30 CARDOZO ARTS & ENT. L.J. 283, 305 (2012) (Although a broad interpretation of the *Sorrell v. IMS Health* majority could be read to mean that all data is speech, "treating all data as speech seems overbroad and highly problematic.").

231. The Free Flow of Information Act of 2013 takes this categorical difficulty into account by protecting not only a "covered journalist," but also allowing for judicial discretion to apply the protections of the shield law to an individual who does not meet the definition of a "covered journalist," when "such protections would be in the interest of justice and necessary to protect lawful and legitimate news-gathering activities under the specific circumstances of the case." S. 987, 113th Cong., 1st Sess. (as reported by S. Comm. On the Judiciary, Nov. 6, 2013).

people, not a vehicle for injecting communication into the 'marketplace of ideas.'"[232]

Without seeking to resolve the debate, this Article assumes that in at least some instances, at least some data processing activities involve speech subject to First Amendment scrutiny. Accepting some data processing as subject to First Amendment analysis merits consideration for the pragmatic reason that firms argue that regulation of information that they collect and exchange interferes with their First Amendment rights.[233]

Even assuming that some data processing is speech subject to First Amendment scrutiny, the state "does not lose its power to regulate commercial activity deemed harmful to the public whenever speech is a component of that activity."[234] In the data processing context, speech is a subordinate component to the firms' ultimate purpose, which is financial gain from transactions in data.[235] Thus, in addition to the worthwhile debate and threshold issue regarding whether all data processing activities are speech, it is also worthwhile to accept as a premise that at least some data processing involves speech and consider whether an opt-in requirement prior to commercial data processing is constitutionally permissible under the First Amendment.

B. The Commercial Speech Doctrine

In 1942, the Supreme Court decided *Valentine v. Chrestensen* holding that commercial speech did not receive First Amendment protection and that prohibition or protection of commercial speech was a legislative matter.[236] Justice Douglas subsequently described the terse *Valentine* decision as "casual, almost offhand. And, it has not survived reflection."[237] In 1976, the Court decided *Virginia State Pharmacy*

---

232. Cohen, *Examined Lives*, *supra* note 6, at 1414.

233. *Id.* at 1375; *U.S. West*, 182 F.3d at 1235, 1235 n. 7 (*citing* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 28–29 (1997)); Tim Wu, *The Right to Evade Regulation: How Corporations Hijacked the First Amendment*, NEW REPUBLIC (June 3, 2013) http://www.newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation.

234. *Ohralik*, 436 U.S. at 456.

235. *See Ohralik*, 436 U.S. at 456–57 (noting that speech is subordinate to the pecuniary interest that motivates in-person solicitation by a lawyer).

236. Valentine v. Chrestensen, 316 U.S. 52 (1942).

237. Cammarano v. United States, 358 U.S. 498, 514 (1959) (Douglas, J., concurring) *superseded by statute*, Revenue Act of 1962, Pub. L. No. 87-834, 29 U.S.C.S. § 162(e)(2) (Lexis), *as recognized in* Cloud v. Commissioner, 97 T.C. 613, 625 (1991). At least one aspect of *Valentine* has survived. In *Valentine*, the Court held that the ban on commercial handbills could not be avoided by adding a non-commercial message to the other side of the paper. 316 U.S. 52. Subsequent commercial speech cases also state that application of the commercial speech doctrine cannot be avoided simply because the commercial speech also includes speech involving an issue of public debate. Bolger v. Youngs Drug

Board v. Virginia Citizens Consumer Council holding that commercial speech is entitled to limited First Amendment protection.[238] While Justice Stewart noted that *Valentine* had been "repeatedly questioned" in the years leading up to *Virginia Pharmacy*,[239] Justice Rehnquist believed that *Valentine* was "constitutionally sound."[240] Rehnquist explained that the "First Amendment speech provision, long regarded by this Court as a sanctuary for expressions of public importance or intellectual interest, is demeaned by invocation to protect advertisements of goods and services."[241] Although Rehnquist's view on *Valentine* did not carry a majority in *Virginia Pharmacy*, the Court has shared his view that commercial speech is deserving of less protection than other types of speech. I argue that properly understood, the commercial speech doctrine can, and should, be applied to protect the privacy interests of individuals against the data processing conduct of online commercial data processors.

1. Defining Commercial Speech

One possible objection to applying the commercial speech doctrine to data processing is that such activity does not fit within the definition of "commercial speech." Case law and scholarship evince disagreement and uncertainty as to the definition of "commercial speech."[242] The *Virginia Pharmacy* Court, quoting an earlier case, defined commercial speech as speech that "does no more than propose a commercial transaction."[243] In *Central Hudson*, the Court defined commercial

---

Prod. Corp., 463 U.S. 60, 67–68 (1983); Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 475 (1989).

238. Virginia State Pharmacy Board v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976). Prior to this decision, Martin Redish published an article that advocated for First Amendment protection of commercial speech. Martin A. Redish, *The First Amendment in the Marketplace: Commercial Speech and the Values of Free Expression*, 39 GEO.WASH. L.REV. 429 (1971). *Virginia Pharmacy Board* is consistent with much of Redish's analysis. At least a couple of student works preceded Redish's article. *See* Tamara R. Piety, *"A Necessary Cost of Freedom"? The Incoherence of Sorrell v. IMS*, 64 ALA. L. REV. 1, 19 & n. 95 (2012) (*citing*, Note, *Freedom of Expression in a Commercial Context*, 78 HARV. L. REV. 1191 (1965); Comment, *Developments in the Law, Deceptive Advertising*, 80 HARV. L. REV. 1005 (1967)) [*hereinafter The Incoherence of Sorrell*].

239. Virginia Pharmacy, 425 U.S. at 776, n.1 (Stewart, J., concurring) (string cite omitted).

240. Bates v. State Bar of Arizona, 433 U.S. 350, 405 (1977) (Rehnquist, J, dissenting) ("The *Valentine* distinction was constitutionally sound and practically workable, and I am still unwilling to take even one step down the 'slippery slope' away from it.").

241. Bates, 433 U.S. at 404 (1977) (Rehnquist, J, dissenting).

242. *E.g.*, Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 61; Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 575 (2001) (Thomas, J., concurring in part and concurring in the judgment) ("I doubt whether it is even possible to draw a coherent distinction between commercial and non-commercial speech.") (*citing* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 523 n. 4 (Thomas, J., concurring in part and concurring in the judgment)).

243. *See Virginia Pharmacy*, 468 U.S. at 762, 771 n. 24 (*quoting* Pittsburgh Press Co. v.

speech as speech that relates "solely to the economic interests of the speaker and its audience."[244] These are narrow definitions of commercial speech.[245] They fail to capture the full scope of speech that ought to be analyzed under the commercial speech doctrine. One reason for this narrow scope of commercial speech as defined by the Court may be that it is a product of the cases before the Court.[246] Additionally, those cases involved older technologies and, therefore, do not reflect a consideration of the limits of what constitutes modern commercial speech.

Erin Bernstein and Theresa Lee raise two points relevant to reconsideration of the scope of the commercial speech definition. First, *Bolger v Youngs Drug Prod. Corp.*[247] is notable because it found that "speech not directly proposing a commercial transaction should be analyzed under the commercial speech doctrine."[248] Second, the definition of commercial speech must be expanded to include the interaction between a data processor and an individual, even when the individual is using the online service for "free."[249] This expansion of the scope of the commercial speech doctrine is not radical.[250] "The

---

Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 385 (1973)).

244. *Cent. Hudson*, 447 U.S. at 561 (*citing* Virginia Pharmacy Board v. Virginia Citizens Consumer Counsel, 425 U.S. 748, 762 (1976); Bates v. State Bar of Arizona, 433 U.S. 350, 363–64 (1977); Friedman v. Rogers, 440 U.S. 1, 11 (1979)).

245. Victor Brudney, *The First Amendment & Commercial Speech*, 53 B.C. L. REV. 1153, 1155 (2012); *but see* Cent. Hudson, 447 U.S. at 579–80 (Stevens, J., concurring in judgment) (the "solely related to the economic interests" definition is "unquestionably too broad" because it includes speech entitled to full First Amendment protection.).

246. Steven Shiffrin, *The First Amendment & Economic Regulation: Away from a General Theory of the First Amendment*, 78 N.W. U. L. REV. 1212, 1213 (1984). In *Nike, Inc. v. Kasky*, the Court had an opportunity to consider whether the definition of commercial speech was broad enough to cover corporate speech regarding a matter of public debate. 539 U.S. 654, 657 (2003). Allegedly, Nike made false statements regarding its labor practices and conditions in its manufacturing facilities. The California Supreme Court held that such speech qualified as commercial speech, even if such speech also played a role in public debate about Nike's labor practices and conditions. 27 Cal. 4th 939, 969 (2002). The Court granted certiorari, however, it subsequently issued a per curiam opinion holding that certiorari had been improvidently granted. Justice Breyer, joined by Justice O'Connor, dissented on the ground that the scope of commercial speech is an important First Amendment issue that the Court should have addressed. *Kasky*, 539 U.S. at 683–84 (Breyer, J., dissenting). For commentary on *Nike v. Kasky*, *see generally*, Symposium: *Nike v. Kasky & The Modern Commercial Speech Doctrine*, 54 CASE W. RES. L. REV. 965 (2004).

247. 463 U.S. 60, 66 (1983).

248. Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 47. The Court found that the "combination" of three factors made the informational pamphlets at issue subject to the commercial speech doctrine: (1) a concession by the speaker that the pamphlets were advertisements; (2) the fact that the pamphlets referenced a specific product; and (3) the fact that the pamphlet provider had an economic motivation for distributing them. Bolger, 436 U.S. at 66–67. The Court expressly stated that none of these three factors alone would be sufficient to invoke review under the commercial speech doctrine. *Id.*

249. Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 75.

250. A radical proposal is that "commercial speech" should cover everything that "for-profit

leveraging of consumer data to sell advertisements or aggregate data is surely as much of a commercial enterprise as providing '(X) good or service at (Y) price.'"[251] However, some question whether the category of commercial speech should be maintained at all, let alone expanded.

Several Justices have expressed concern that truthful, non-misleading commercial speech does not receive the same protection as non-commercial speech.[252] Commentators have asserted that distinguishing between commercial and non-commercial speech "makes no sense."[253] Another commentator believes that increasing media convergence and the rise of user-generated content create practical and principled problems in maintaining a dichotomy between commercial and non-commercial speech.[254] To be sure, distinguishing commercial speech from other fully protected speech is sometimes complex.[255] But, it is not an impossible task. Indeed, making such distinctions is how lawyers and judges earn their keep.

As Bernstein and Lee noted, the creation of profiles and online behavioral advertising by commercial actors are no less commercial than a pharmacy advertising drug prices. In both instances, the commercial activities are motivated by economic gain.[256] As Thomas

---

entities say, because no matter how it appears, no matter what communicative form it assumes, communications by for-profit entities are always and essentially promotional and hence 'commercial,' because for-profit corporations have no other purpose for being under the law (at least in the United States under current law)." TAMARA R. PIETY, BRANDISHING THE FIRST AMENDMENT: COMMERCIAL EXPRESSION IN AMERICA 12 (2012). Piety's proposal is radical in the sense that it deviates significantly from the Court's commercial speech jurisprudence, not that it is an unreasonable proposal.

251. Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 76 (citing David F. McGowan, *A Critical Analysis of Commercial Speech*, 78 CALIF. L. REV. 359, 401 (1990)). Bernstein and Lee further support the modest nature of their proposal by drawing an analogy to courts finding that clickwrap and even browsewrap agreements as enforceable contracts. Courts would not find these to be enforceable if no value was exchanged. Id. at 77–78.

252. Lorrilard Tobacco, 533 U.S. at 571–72 (Kennedy, concurring in part and concurring in the judgment); Greater New Orleans Broadcasting Ass'n v. United States, 527 U.S. 173, 197 (1999) (Thomas, J., concurring in judgment); Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 432–38 (1993) (Blackmun, J., concurring); *see*, Cent. Hudson, 447 U.S. at 583 (Stevens, J., concurring in the judgment) (does not believe *Central Hudson* involved "commercial speech"); *and* Rubin v. Coors Brewing Co., 514 U.S. 476, 493–97 (1995) (Stevens, J., concurring).

253. Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627, 628 (1990).

254. Adam Theier, *Advertising, Commercial Speech, and First Amendment Parity*, 5 CHARLESTON L. REV. 503, 506 (2011).

255. Virginia Pharmacy, 425 U.S. at 784 (Rehnquist, J., dissenting).

256. While financial motivation alone cannot dispositively establish speech as commercial, by definition, the economic incentive of the speaker must be a factor. Bolger, 463 U.S. at 67. In addition to *Bolger*, other Supreme Court commercial speech decisions show that the economic motivation of a speaker is a relevant factor identifying and analyzing commercial speech. *E.g.*, In Re Primus, 436 U.S. 412 (1978); *and* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978).

In *Ohralik*, the Court upheld a ban on in-person solicitation by lawyers because the pecuniary incentive created a risk to substantial state interests in protecting privacy and preventing undue influence. Ohralik,

Emerson noted, changing societal conditions require reconsideration of existing law regarding free expression.[257] If the current definition of commercial speech does not include data processing by commercial actors, then the definition ought to be expanded to include this substantial area of our information economy,[258] especially when considering the original purpose of the commercial speech doctrine.

2. Purpose of the Commercial Speech Doctrine

The *Virginia Pharmacy* Court did not protect commercial speech for the purpose of protecting the commercial speaker's interest in financial gain. Rather, commercial speech was protected for individual and societal interests in facilitating the ability of individuals to make informed decisions and improve competition in the marketplace.[259] In assessing the validity of a commercial speech regulation the Court stated, "The listener's interest in substantial."[260] But, not all commercial speech furthers these individual and societal interests. Two examples help illustrate this point.

First, not all commercial speech is informational. The speech in *Virginia Pharmacy* is a quintessential example of purely informational speech. The Court described the speech as, "I will sell you the X prescription drug at the Y price."[261] Purely informational speech serves the individual and societal interests underlying the commercial speech doctrine. Propaganda or persuasive speech, however, may actually harm these interests. Although there is no clear line between purely informational speech and propaganda, that is not a reason for the law to decline to acknowledge these as distinct points on a continuum and seek to craft legal standards that do not equate commercial speech with core First Amendment speech.[262]

---

436 U.S. at 449, 461–62. In *Primus*, the Court noted the lack of pecuniary gain as a relevant factor in prohibiting the suppression of speech by an attorney soliciting pregnant mothers on public assistance in South Carolina that were sterilized or being threatened with sterilization. In re Primus, 436 U.S. at 422. The Court applied "exacting" scrutiny because the speech in this case involved "core First Amendment rights." Id. at 432. The *Primus* Court noted that the purpose or motive of the speaker is relevant in a commercial speech analysis, even though such analysis is not normally at the center of First Amendment analysis. Id. at 438, n.2.

257. Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 894–95 (1963).

258. For an early scholarly exploration of the implications of the information economy on privacy rights, *see e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 192 (1992).

259. Bates, 433 U.S. at 364; Cent. Hudson, 447 U.S. at 574 (Blackmun, J., concurring).

260. Bates, 433 U.S. at 364.

261. Virginia Pharmacy, 468 U.S. at 761.

262. *See*, Florida Bar v. Went For It, Inc., 515 U.S. 618, 623 (1995) ("We have always been careful to distinguish commercial speech from speech at the First Amendment's core.").

Second, sometimes the method in which commercial speech is received may be counterproductive to the individual and societal interests that the commercial speech doctrine seeks to protect. As the Court has stated, "the mode of communication makes all the difference."[263] In *Bates v. State Bar of Arizona*,[264] a newspaper advertisement displaying prices for routine legal services received First Amendment protection. In *Ohralik v. State Bar Association*,[265] however, an in-person solicitation by a lawyer while the potential client was in the hospital immediately after a car accident crossed the line. The Court viewed this method of solicitation as overreaching and not protected by the First Amendment. In addition to overreaching, the Court was concerned that an in-person solicitation presented unique regulatory challenges because it is "not visible or open to public scrutiny."[266] Thus, in-person solicitation "actually may disserve the individual and societal interests, identified in *Bates*, in facilitating 'informed and reliable decision-making.'"[267]

Data processing is somewhat analogous to in-person solicitation because firms' data processing practices are not visible or open to public scrutiny. Individuals generally do not know what information is being collected, how it's used, or with whom its shared. Online behavioral advertising raises similar concerns as in-person solicitation. Commercial actors are targeting specific advertisements at specific individuals based on profiles and may be viewed as overreaching, especially when they use these profiles to engage in price discrimination

263. Shapero v. Kentucky Bar Ass'n, 486 U.S. 466, 475 (1988) (holding that a ban on all direct mail solicitation by lawyers violated the First Amendment). Although *Shapero* does not find targeting advertisements via mail problematic, it could not have foreseen the exponential advances in a commercial actor's ability to target individuals. Thus, while *Shapero* must be addressed in assessing the legitimacy of an opt-in requirement, it should not be viewed as dispositive because it could not have foreseen the unique challenges of online data processing in 1988. *See* Part II.A, above.

264. 433 U.S. 350 (1977).

265. 436 U.S. 447 (1978).

266. Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio, 471 U.S. 626, 641 (1985) (*quoting* Ohralik, 436 U.S. at 466).

267. Ohralik, 436 U.S. 444, 457–58 (1978). In *Edenfield v. Fane*, the Court held a Florida statute prohibiting in-person solicitation by Certified Public Accountants (CPAs) as unconstitutional in violation the First Amendment. 507 U.S. 761 (1993). On the surface, *Edenfield* may suggest that in-person solicitation itself is not problematic and therefore provide a counterpoint to my argument that data processing is problematic because it is somewhat analogous to in-person solicitation. *Edenfield* is distinguishable for two reasons. First, Florida failed to provide evidence of actual harm caused by in-person solicitations by CPAs. As set forth in this Article, there is evidence of harm. See Part II.A, above, and IV.B.6, below. Second, the Court noted that the in-person solicitations occurred at the business offices of sophisticated listeners, and only if they agreed to the solicitation. Data processing is fundamentally different because it involves less sophisticated parties and intrudes further into an individual's life than an infrequent solicitation by a CPA at the solictee's business office.

or other activities that are harmful to individuals.[268] An opt-in requirement helps remedy the lack of transparency and overreaching.

While online behavioral advertising is not as intrusive as when a lawyer seeks to solicit an accident victim in the hospital, online behavioral advertising is not as innocuous as the newspaper advertisement upheld in *Bates*. In the commercial speech context, the Court has noted that "an untargeted letter mailed to society at large is different in kind from a targeted solicitation."[269] Additionally, the FTC has recognized the detrimental aspects of in-person solicitation in the context of ordinary consumer products,[270] as well as the detrimental aspects of online data processing.[271] To the extent that online commercial data processing disserves the individual and societal interests in fostering informed and reliable decision-making, such activity may be regulated commercial speech. Or, at least such speech is not supported by the original purpose of the commercial speech doctrine.

In the attorney speech context and beyond, several Supreme Court commercial speech decisions have been sensitive to the medium of communication in analyzing the permissibility of the regulation. On numerous occasions, the Court has expressly excluded "electronic broadcast media" from the scope of its decisions because of the "special problems" created by this technology.[272] As set forth in Part II and as acknowledged by the Supreme Court,[273] online data processing raises unique and unresolved challenges to individual privacy interests. Thus, while prior commercial speech case law in the offline context is relevant in analyzing the permissibility of an opt-in requirement for online data processing, the Court has expressly left open the possibility that different technology platforms may require different commercial speech

---

268. *See also*, Latanya Sweeney, *Discrimination in Online Ad Delivery* at 34 (2013) (Without identifying the specific cause(s), Sweeny's study found that "[a] greater percentage of ads having 'arrest' in ad text appeared for black identifying first names than for white identifying first names in searches on Reuters.com, on Google.com, and in subsets of the sample."), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240.

269. Florida Bar v. Went For It, Inc., 515 U.S. at 630. In a prior case, the Court held that targeted mailings alone are an insufficient reason to suppress commercial speech. Shapero v. Kentucky Bar Ass'n, 486 U.S. 466 (1988). *Shapero* is distinguishable because online data processing is not functionally identical to an isolated mailing sent to an individual whose home is in foreclosure. *See* Part I, above.

270. Ohralik, 436 U.S. at 464.

271. *See* Part II, above, and accompanying notes.

272. Virginia Pharmacy, 468 U.S. at 773; Bates, 433 U.S. at 384; Cent. Hudson, 447 U.S. at 576 (Blackmun, J., concurring in the judgment); Zauderer 471 U.S. at 673, n.1 (O'Connor, J., concurring in part, concurring in the judgment in part, dissenting in part) (noting that neither the majority nor her and those joining her opinion express any views on whether the rule announced for attorney advertising in newspapers applies to electronic broadcast media).

273. Sorrell v. IMS Health, 131 S. Ct. 2653, 2672 (2011).

rules.[274]

An opt-in requirement is consistent with the purpose of protecting individuals' interests in the commercial speech context. Data processors have an economic incentive not to be forthcoming about their data processing practices or to provide an individual the ability to opt-out, let alone offer an opt-in approach. Individuals are not well situated to force such disclosures.[275] In other words, there is a market failure, in large part, because of substantial information asymmetry and power discrepancy. When markets fail, government regulation is a traditional response.[276] A legislatively required opt-in mechanism prior to data processing is such a response and it serves the purpose of the commercial speech doctrine because it protects individual and societal interests in the context of commercial activity.

3. Justifications for Limited First Amendment Protection

The Court did not simply state that the purpose of the commercial speech doctrine was to protect individual and societal interests. It also provided two primary justifications for why commercial speech could withstand less than full First Amendment protection. First, commercial speech is more durable than other speech because it is the result of the economic interests of the commercial actor.[277] Speech motivated by financial gain is less likely to be chilled than other speech.[278] Second, commercial speech does not need as much protection as other speech because truth is more readily verifiable by the seller of goods or services than speech in non-commercial contexts.[279] These justifications are not without detractors.

Some commercial speech, such as the health effects of eggs, may be less verifiable than political speech by a candidate, such as the truth about his past.[280] Some non-commercial speech may be as hardy as or

---

274. Not all Justices agree that the First Amendment protections may vary based on the technology used to communicate speech. *See e.g.*, FCC v. Fox Television Stations, Inc., 556 U.S. 502, 530–35 (2009) (Thomas, J., concurring).

275. Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 67.

276. SIDNEY SHAPIRO & JOSEPH P. TOMAIN, ACHIEVING DEMOCRACY: THE FUTURE OF PROGRESSIVE REGULATION xiii (2014).

277. Virginia Pharmacy, 425 U.S. at 772, n. 24; Bates, 433 U.S. at 771–72; Cent. Hudson, 447 U.S. at 564, n. 6; Fox, 492 U.S. at 482.

278. Virginia Pharmacy, 425 U.S. at 772, n. 24; Cent. Hudson, 447 U.S. at 564, n. 6.; Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985) (speech "solely motivated by the desire for profit . . . is a force less likely to be deterred than others.").

279. Virginia Pharmacy, 425 U.S. at 777–78 (Stewart, J., concurring); Bates, 433 U.S. at 383.

280. Daniel Farber, *Commercial Speech and First Amendment Theory*, 74 NW. U.L. REV. 372, 385–86 (1979); Steven Shiffrin, *The First Amendment and Economic Regulation: Away from a General*

hardier than commercial speech, such as religious speech.[281] These critiques of the justifications for affording commercial speech with less than full First Amendment protection are not unwarranted. Modern advertising techniques have gone far beyond merely providing purely informational speech, such as the prices of drugs at issue in *Virginia Pharmacy*.[282] History shows that religious speech is at least as hardy as commercial speech, if not more, and it is provided full First Amendment protection. But, even if these justifications for affording commercial speech less protection are wanting, that does not prove that commercial speech should be afforded full First Amendment protection.

First, that advertising techniques have gone far beyond the simple provision of factual information actually supports limited First Amendment protection of commercial speech. *Virginia Pharmacy* protected purely informational speech, the price of drugs. It did not address speech that aims to persuade. Justice Rehnquist worried about the ramifications of *Virginia Pharmacy* on commercial speech that aims to persuade.[283] He worried that *Virginia Pharmacy* would be used to extend First Amendment protection to such speech. Because of the vast information asymmetry between individuals and data processors, individuals are at risk of manipulation, especially when professional marketers engage in speech aimed to persuade.[284]

Second, the critique of the durability justification does not disprove the durability of commercial speech; it merely shows that other speech may be as durable or more durable. Even accepting this critique, it does not prove that commercial speech is entitled to full First Amendment protection. For example, religious freedom is expressly protected by the Constitution, unlike commercial speech, and that may be a reason for not affording commercial speech full First Amendment protection, even though religious speech is equally or more durable. Similarly, there is near universal agreement that the First Amendment protects political speech. Even though commercial speech may be no less durable than political or religious speech, commercial speech does not share the historical or textual protection afforded to these speech categories.

Another justification provided by the Court for limiting the First Amendment protection afforded to commercial speech goes to First Amendment theory and jurisprudence. A common theory that has been

---

Theory of the First Amendment, 78 NW. U.L. REV. 1212, 1218 (1983); Kozinksi & Banner, *Who's Afraid of Commercial Speech?*, *supra* note 253, at 637.

281. Kozinksi & Banner, *Who's Afraid of Commercial Speech?*, *supra* note 253, at 637; Martin Redish, *The Value of Free Speech*, 130 U. PA. L. REV.591, 633 (1982).

282. Kozinski & Banner, *Who's Afraid of Commercial Speech?*, *supra* note 253, at 635–36.

283. Virginia Pharmacy, 425 U.S. at 788 (Rehnquist, J., dissenting).

284. *See e.g.*, Calo, *Digital Market Manipulation*, *supra* note 2.

recognized in Supreme Court case law is that the solution to problematic speech is more speech.[285] In the commercial speech context, however, the Court has recognized that the theory does not work in practice.[286]

4. Whose Right to Receive Information?

The commercial speaker's right to receive information is a novel question in the commercial speech context. *Virginia Pharmacy* focused on the public's right to receive information about drug prices; it does not address the commercial speaker's right to receive information.[287] An opt-in requirement does not keep the public ignorant. To the contrary, an opt-in requirement supports the public's right to receive information by alerting consumers as to how their personal data can be used. The holding in *Virginia Pharmacy* should not be twisted into an argument that an opt-in requirement violates a commercial actor's right to receive information because the right of the commercial actor to receive information is not equivalent to the public's right to receive information in the commercial speech context. Indeed, the reasoning of *Virginia Pharmacy* where the Court overturned a speech suppressing law actually supports the Vermont law overturned in *Sorrell*, even though that law suppressed information.

In *Virginia Pharmacy*, the Court protected the commercial speech at issue by citing the citizen-consumer's right to receive information.[288] The Court reasoned that suppressing the price of drugs has the most detrimental effect on vulnerable populations, such as the poor, the sick and elder populations.[289] The Court was concerned that the advertising ban created risks of excessive prices and inferior service because it kept "citizens" ignorant.[290]

The concern regarding protecting vulnerable populations also arises in *Sorrell*. The Vermont law sought to protect patients from the effects

---

285. *See e.g.*, United States v. Alvarez, 132 S. Ct. 2537 (2012) (*quoting* Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

286. Ohralik, 436 U.S. at 457; Cent. Hudson, 447 at 598 (Rehnquist, J., dissenting).

287. Other commercial speech cases also focus on the public's right to receive information. *E.g.* Bolger, 463 U.S. at 79 (Rehnquist, J., concurring in the judgment); 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 503 (1996). Further, non-commercial speech cases also focus on the public's right to receive information. *See e.g.* Red Lion Broad. v. FCC, 395 U.S. 367, 390 (1969) ("It is the right of the listeners and viewers that is paramount, not the broadcasters"); *and,* Procunier v. Martinez, 416 U.S. 396, 409–10 (1974) (prison rules restricting inmate correspondence abridged non-inmate recipients' First Amendment rights).

288. Virginia Pharmacy, 425 U.S. at 756–57. Rehnquist disputed that the case centered on the listener's right to receive information. He viewed the issue as the right of a party to publish information. Id. at 782.

289. Virginia Pharmacy, 425 U.S. at 763.

290. Virginia Pharmacy, 425 U.S. at 769.

of pharmaceutical companies "hawking"[291] their higher-priced brand-name drugs as alternatives to generics and the risk of physicians overprescribing drugs.[292] Patients being prescribed drugs are a vulnerable population because they do not have the expertise of the prescribing physicians, they are not privy to the marketing communications that the physicians hear, and they do not have the data that the detailers or pharmaceutical companies use to craft their pitch. Thus, in the commercial speech context, a commercial speaker's right to receive information should be viewed as a subordinate concern when compared to the interests in protecting citizens.

Despite *Sorrell* (and *Citizens United v. FEC*[293]), the identity of the party is (or should be) relevant when analyzing the right to receive information, at least in the commercial speech context. Indeed, the Court has expressly stated that the identity of the parties matter when analyzing whether a ban on in-person solicitation is a constitutional regulation of commercial speech.[294] And, suppression of information alone is an insufficient factor to assess the validity of a commercial speech regulation.

In *Virginia Pharmacy*, the Court was concerned that *too little* information in the hands of the listening public would be detrimental to their interests in being able to make informed decisions regarding drug prices. In *Sorrell*, Vermont was concerned that *too much* information in the possession of speakers motivated primarily or "purely"[295] by economic gain would be detrimental to the interests of patients being prescribed drugs. By prohibiting detailers and pharmaceutical companies from receiving prescribing physicians' data, Vermont was not seeking suppress information from citizen-consumers. Vermont was

---

291. Justice Rehnquist did not believe that the Founding Fathers would have viewed regulation of economic activity, including advertising, as beyond the scope of state regulation:

> Nor do I think those who won our independence, while declining to 'exalt order at the cost of liberty,' would have viewed a merchant's unfettered freedom to advertise in hawking his wares as a 'liberty' not subject to extensive regulation in light of the government's substantial interest in attaining 'order' in the economic sphere.

Cent. Hudson, 447 U.S. at 595 (Rehnquist, J., dissenting).

292. The Court described "detailing" as "an expensive undertaking, so pharmaceutical companies most often use it to promote high-profit brand-name drugs protected by patent." Sorrell, 131 S. Ct. at 2660.

293. Citizens United v. Federal Election Comm'n, 558 U.S. 310 (2010). *Citizens United* held that the Bipartisan Campaign Reform Act violated the First Amendment rights of corporations and unions because it discriminated based on the identity of the speaker in the context of political speech. Id. at 341.

294. Edenfield, 507 U.S. at 774; *see also*, Went For It, 515 U.S. at 636 (Kennedy, J., dissenting) ("Speech has the capacity to covey complex substance, yielding various insights and interpretations depending upon the identity of the listener or the reader and the context of its transmission.").

295. In *Virginia Pharmacy*, the Court assumed that the "advertisers interest is a purely economic one." 425 U.S. at 762.

seeking to further the interests that supported *Virginia Pharmacy*. Namely, Vermont was seeking to avoid excessive charges and inferior service that would result from doctors prescribing higher priced name-brand drugs instead of generic alternatives and overprescribing drugs.

In sum, neither the right to receive information nor the suppression of information in the abstract is the *sine qua non* of commercial speech analysis. The *sine qua non* is the public interest.[296] While the right to receive information and the suppression of information are factors in determining the public interest in commercial speech, another important factor in commercial speech analysis is whether the regulation seeks to keep the *public* in the dark.[297] In *Virginia Pharmacy*, the law kept the public ignorant about drug prices, which operated to their detriment. In *Sorrell*, the law was intended to keep the commercial actor in the dark regarding a physician's prescribing practices to prevent the economic actor from taking advantage of information to the possible harm of the patient merely because it is in the commercial actor's economic interests to do so. As the *Sorrell* Court noted, in the medical profession and more generally, "information is power."[298] Because the interests of the commercial speaker are not at the core of commercial speech doctrine, it is at least an open question whether keeping the commercial actor in the dark raises the same concerns as keeping the public ignorant of information.

As Ryan Calo has observed in the behavioral economics context, information has played a variety of roles in human history. Information has been the hero, the villain, and most recently, the victim.[299] In the commercial speech context, the complex nature of information should not be overlooked. The identity of the party being denied information should play a role in assessing the validity of a regulation that keeps a party in the dark because an individual-listener's interest in receiving information is not equivalent to a commercial-speaker's interest.

---

296. In *Virginia Pharmacy*Public Citizen argued that commercial speech merited constitutional protection to the extent that it benefited the public. Brief of Appellees, Virginia State Board of Pharmacy v. Virginia Citizens Council, Inc., 1975 WL 173826, *10 (1975) (The public have "an independent right to receive drug information which is not derivative from the rights of speakers to disseminate that information."). *See also* Haley Sweetland Edwards, *The Corporate "Free Speech" Racket: How corporations are using the First Amendment to destroy government regulation*, WASH. MONTHLY (January/February 2014).

297. *See* 44 Liquormart, 517 U.S. at 503 ("The First Amendment directs us to be especially skeptical of regulations that seek to keep people in the dark for what the government perceives to be their own good."); Id. at 526 (Thomas, J., dissenting) ("all attempts to dissuade legal choices by citizens by keeping them ignorant are impermissible.").

298. Sorrell, 131 S. Ct. at 2671 (quoting a Vermont physician).

299. Calo, *Digital Market Manipulation*, *supra* note 2, at 1012–14. Information can be a villain because of information overload, a hero because more information can lead to better choices, and a victim because of the privacy intrusions caused by Big Data. *Id.*

5. Disclosure Laws versus Speech Suppressing Laws

A disclosure requirement is a necessary component of an opt-in regime that aims to allow for informed consent. Early in the Court's commercial speech jurisprudence, it recognized the possibility that a disclosure requirement might be necessary in some instances to prevent consumers from being misled.[300] Not long thereafter, in *Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio*,[301] the Court upheld a disclosure requirement in the context of attorney advertising. The Court held that a disclosure need only be "reasonably related to the State's interest in preventing deception of consumers."[302]

This holding appears to create an even lower threshold for commercial speech regulation requiring a disclosure, as opposed to *Central Hudson's* intermediate scrutiny standard when the law imposes a prohibition on speech.[303] In upholding the disclosure requirement, the *Zauderer* Court noted that its commercial speech jurisprudence has consistently viewed disclosure requirements as a less restrictive alternative to suppressing speech altogether.[304] The Court reasoned that a lower threshold for disclosure requirements is warranted because a commercial speaker has "substantially weaker" First Amendment interests in being compelled to disclose truthful information than in being suppressed from speaking.[305] This view is particularly true in the commercial speech context where the commercial actor is simply required to disclose verifiable information about its product or service to avoid consumer deception or overreaching.[306] At least one Justice believed that disclosure requirements do not even involve the commercial speech doctrine because laws that seek to protect "consumers from incomplete information" are permissible.[307] And in *Sorrell*, one reason Justice Breyer dissented from the Court's use of "heightened" scrutiny was because the Vermont law did not require or

300. Bates, 433 U.S. at 384.

301. Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio, 471 U.S. 466 (1985).

302. Zauderer, 471 U.S. at 651. The specific requirement upheld was the disclosure that in a contingency fee arrangement, the client may be responsible for costs, even if the case is lost. Id. at 652.

303. *Id.* In his *Zauderer* concurrence, Justice Brennan joined by Justice Marshall, stated that disclosure requirements should be subject to the same level of review as commercial speech regulations that prohibit speech. *Id.*at 657–58 & n. 1 (Brennan, J., concurring in part, concurring in the judgment in part, dissenting in part).

304. *Id.* at 651, n. 14.

305. Id. at 651, n.14; In re R.M.J., 455 U.S. 191, 203 (1982).

306. See Zauderer, 471 U.S. at 651, n.14 ("The right of a commercial speaker not to divulge accurate information regarding his services is not such a fundamental right.").

307. Rubin, 514 U.S. at 491–92 (Stevens, J., concurring).

forbid the detailers or pharmaceutical companies saying anything.[308]

A disclosure requirement as to what data is collected, how it's used, and with whom it's shared is directly related to informing consumers and is reasonably related to preventing consumer deception. Of course, there could be a disclosure requirement without an opt-in feature, if the Court or Congress viewed disclosure of data processing practices as sufficient to protect the individual's interests. Because an opt-in regime seeks to do more than simply prevent individuals from being misled, however, providing consumers the option to refuse to consent to data processing is essential. In addition to preventing individuals from being misled as to a commercial actor's data processing practices, an opt-in requirement protects the privacy interests set forth in Part II, helps prevent the commodification of human beings, and avoid other harms such as price discrimination, and adverse insurance or employment decisions based on statistical inferences.

6. Applying *Central Hudson* to an Opt-In Requirement

Once speech has been deemed "commercial speech," the Court must consider whether a regulation of that speech violates the First Amendment. In *Central Hudson*, the Court set forth a four-part test to make this determination. First, the speech must "at least concern lawful activity and not be misleading."[309] Second, the government interest supporting the regulation of the speech must be "substantial."[310] Third, the Court analyzes whether the regulation "directly advances" the governmental interest.[311] Finally, the regulation must not be "more extensive than is necessary to serve that interest."[312]

Subsequent to *Central Hudson*, the Court clarified the contours of the third and fourth factors. The third factor means that the regulation directly advances the governmental interest in a "material way."[313] The fourth factor does not require that the regulation be the "least restrictive" means for serving the interest.[314] Rather, there must be a "reasonable fit" between the regulation and the interest served.[315] In other words, the *Central Hudson* test is one of intermediate, not strict scrutiny.[316]

---

308. Sorrell, 131 S. Ct. at 2673 (Breyer, J., dissenting).

309. Cent. Hudson, 447 U.S. at 566.

310. Id.

311. Id.

312. Id.

313. Edenfield v. Fane, 507 U.S. 761, 767 (1993).

314. Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 476 (1989) (the fourth-prong of *Central Hudson* "requires something short of a least-restrictive-means standard.").

315. Fox, 492 U.S. at 480.

316. Went For It, Inc., 515 U.S. 618, 624 (1995).

Some Justices have questioned whether intermediate scrutiny is sufficient protection for truthful, non-misleading commercial speech.[317]

Under a faithful application of the *Central Hudson* test, legislation requiring data processors to receive an individual's express, affirmative, and informed opt-in consent prior to data processing should survive First Amendment review. First, while there could be debate about whether data processors engage in misleading behavior in the ways they process data, such as hidden web bugs or intentionally opaque terms of service, I do not engage in that analysis here. Data processing is presumed lawful and non-misleading for purposes of this Article.

Second, several state interests that the Court has accepted as substantial are applicable to an opt-in requirement. Protecting individual privacy is a substantial interest.[318] Although the *Sorrell* Court rejected the argument that a purpose of the Vermont law was to protect individual privacy, it stated: "Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers."[319] In the context of in-person solicitations by lawyers shortly after an accident, the Court noted that uninvited solicitations may "distress the solicited simply because of their obtrusiveness and the invasion of individual privacy, even when no other harm materializes."[320] Unconsented-to data processing invades privacy because of the creation of profiles and tracking of individual's internet activity. Online behavioral advertising can also be described as an uninvited and obtrusive solicitation that invades individual privacy. If the reasoning in *Ohralik* is applied in this context, then it is not necessary to identify other harms because individual privacy is a substantial state interest and the intrusiveness of unconsented-to data processing invades that interest. But, there are other harms that the Court has acknowledged as substantial state interests worthy of protection in the commercial speech context.

Preventing undue influence, overreaching, and misrepresentation are all substantial state interests, according to the Court.[321] Solicitations can be regulated to protect individuals from such risks.[322] Many of the Court's solicitation cases acknowledge the special concerns that arise when an attorney uses his "professional expertise to overpower the will

317. Central Hudson, 447 U.S. at 573 (Blackmun, J., concurring in the judgment); Lorillard Tobacco Co., 533 U.S. at 572 (Thomas, J., concurring in part and concurring in the judgment) (conceding that *Central Hudson* imposes an intermediate scrutiny standard, but stating that strict scrutiny should apply to all truthful "commercial" speech).

318. In re Primus, 436 U.S. at 432; Ohralik, 436 U.S. at 461; Edenfield, 507 U.S. at 769.

319. Sorrell, 131 S. Ct. at 2672.

320. Ohralik, 436 U.S. at 465–66.

321. Bates, 433 U.S. at 366; In re Primus, 436 U.S. at 432; Ohralik, 436 U.S. at 462.

322. Ohralik, 436 U.S. at 462.

and judgment of lay people who have not sought their advice."[323] Similar concerns arise in the context of data processing because advertisers are seeking to use their professional expertise in the "art of persuasion"[324] to overcome the will of lay people that have not chosen to be targeted or profiled. An opt-in requirement helps ameliorate these risks.

One final state interest recognized by the Court may be extrapolated to the data processing context: commercial exploitation of individuals. In *Fox*, the Court held that commercial exploitation of college students was a substantial state interest.[325] This state interest could be expanded to apply to data processing, regardless of whether one is a college student. An opt-in requirement helps avoid the commercial exploitation of individuals in a situation of great information asymmetry and power disparity.

Third, in establishing that the regulation advances the state interest in a direct and material way, the government "must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[326] Although the government must do more than provide a conclusory assertion that the regulation will directly and materially advance the state interest, it need not prove actual harm, nor provide empirical evidence.[327] Prophylactic rules to prevent harms stemming from solicitation are permissible.[328] Because an opt-in requirement is a prophylactic rule designed to prevent harm before it occurs, proof of actual harm should not be required. With that said, there is proof of harm resulting from data processing beyond the obtrusive nature of uninvited solicitations.

---

323. Zauderer, 471 U.S. at 678 (O'Connor, J., concurring in part, concurring in the judgment in part, dissenting in part); Shapero, 486 U.S. at 474 ("The relevant inquiry is . . . whether the mode of communication poses a serious danger that lawyers will exploit any such susceptibility [to undue influence].").

324. Edenfield, 507 U.S. at 775 (noting that a CPA, unlike a lawyer, is not a "professional trained in the art of persuasion). Like lawyers, however, online advertisers that use profiles to target advertising at individuals are trained in the art of persuasion. *See generally*, PACKARD, HIDDEN PERSUADERS, *supra* note 15; *and*, TUROW, DAILY YOU, *supra* note 4.

325. Fox, 492 U.S. at 475.

326. Edenfield, 507 U.S. at 770–71.

327. Lorillard Tobacco, 533 U.S. at 555.

328. Ohralik, 436 U.S. at 464. Although *Edenfield*, limited the application of prophylactic rules to regulate commercial speech, it did not prohibit them. Edenfield, 507 U.S. at 774–76. In *Edenfield*, the Court struck down Florida's prohibition on in-person solicitation by certified public accountants because no studies or anecdotal evidence was submitted. Edenfield, 507 U.S. at 771. In *Florida Bar v. Went For It*, the Court upheld the Florida Bar's ban on direct mail solicitation of personal injury or wrongful death clients within 30 days of the accident. 515 U.S. 618 (1995). Unlike the lack of evidence in *Edenfield*, the Florida Bar provided a 106-page summary based on a two year study regarding the effects of lawyer advertising on public opinion of the profession and significant anecdotal evidence. Went for It, 515 U.S. at 626–28.

There is evidence to support that an opt-in regime will advance the privacy interests of individuals. Consumer survey studies by Joseph Turow and others show a clear consumer preference for less uninvited data processing.[329] Starting over fifteen years ago, the FTC has issued multiple reports regarding online privacy concerns raised by online data processing. In 2012, the White House issued its privacy bill of rights in response to online privacy concerns. In 2013, a Senate Subcommittee Report concluded data processing without consent will continue if the status quo is maintained.[330] An opt-in requirement directly advances these privacy interests in a material way because it empowers the individual to make an express, affirmative, and informed choice about whether to forego her privacy prior to data processing. An opt-in requirement helps restore at least some information symmetry in the interaction between the individual and the data processor. Currently, data processors are incentivized to be less than forthcoming in their data processing practices and to make it difficult to opt-out, if there is any option at all.

Under the final prong of the *Central Hudson* test, the regulation need not be the least restrictive means. Rather, it must be a "reasonable fit" between interests being protected and the means of protecting them. There is a reasonable fit between the privacy interests and an opt-in requirement. A necessary component of an opt-in regime is a disclosure requirement. The disclosure requirement must inform individuals about the firm's data processing practices. In analyzing commercial speech regulations, the Court has stated that disclosure requirements are often noted as being a less restrictive regulation than a prohibition on speech.[331]

Moreover, an opt-in requirement is not a complete ban on data processing. An opt-in requirement merely requires that data processors receive meaningful consent from an individual before engaging in data processing. If an individual prefers to receive behavioral advertising or believes that profiles created by data aggregators inure to her benefit, then such a choice is perfectly legal under this proposal. In other words, an opt-in requirement is a nudge that seeks to respect the probable preferences of individuals, while still allowing data processing to occur after the commercial actor receives the individual's meaningful consent. An opt-in requirement should pass constitutional muster under the

329. Joseph Turow, et al., *Americans Reject Tailored Advertising & Three Activities that Enable It*, Sept. 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

330. SENATE COMM. REPORT, *supra* note 124, at 35.

331. Zauderer, 471 U.S. at 651, n. 14 ("all our discussions of restraints on commercial speech have recommended disclosure requirements as one of the acceptable less restrictive alternatives to actual suppression of speech.").

Central Hudson formulation of the commercial speech doctrine.

C. Erosion and Inversion of the Commercial Speech Doctrine

At the same time that advertising is increasingly permeating our lives,[332] the Court has eroded the ability of the commercial speech doctrine to regulate economic activity that has (at least ostensibly) a speech component.[333] Some lament this erosion, while others celebrate it arguing that the Court has not gone far enough until commercial speech is treated no differently than non-commercial speech.[334] I fall decidedly on the side of those who lament the erosion of the commercial speech doctrine.

Not only is the Court eroding the commercial speech doctrine, its decision in *Sorrell v. IMS Health* "turned that doctrine on its head."[335] The Court has turned the commercial speech doctrine on its head because the doctrine was intended to protect the interests of listeners, not the interests of the commercial speakers. *Sorrell* focused on protecting the interests of commercial actors.

In *Sorrell*, a state law limited the collection, use, and sale of a physician's prescribing history by pharmaceutical companies and "detailers,"[336] unless the physician opted-in. The Court referred to multi-billion dollar pharmaceutical companies and detailers as "disfavored" speakers because others, such as researchers, could use the same data without having to receive the physician's consent. The Court described the content regulated by the statute as "disfavored" because the statute sought to limit pharmaceutical marketing speech, or more precisely the data accessible to detailers and pharmaceutical companies. For these reasons, the Court determined that "heightened scrutiny" was

---

332. PIETY, BRANDISHING THE FIRST AMENDMENT, *supra* note 250, at 49 ("We cannot avoid the visual clutter of billboards, or the promotional tie-ins to movies or other entertainment in stores, restaurants, and the culture at-large.").

333. *Id.* at 223 ("the rhetoric in those cases suggests that increased protection for commercial speech is almost inevitable."); Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 51 ("the outcome of [*Sorrell*] left many questioning the continued viability of the commercial speech doctrine"); Purdy, *Roberts Court v. America*, *supra* note 223, at 50 (noting the Court's "growing protection for business's commercial speech"); Jennifer L. Pomeranz, *No Need to Break New Ground: A Response to the Supreme Court's Threat to Overhaul the Commercial Speech Doctrine*, 45 LOYOLA L.A. L. REV. 389, 398 (2012).

334. *E.g.*, Kozinksi & Banner, *Who's Afraid of Commercial Speech?*, *supra* note 253; Adam Thierer, *Advertising, Commercial Speech, and First Amendment Parity*, 5 CHARLESTON L. REV. 503 (2011); Lorillard Tobacco, 533 U.S. at 554 (noting that the petitioners in the case before the Court, as well as parties in prior cases have advocated for replacing *Central Hudson's* intermediate scrutiny with a strict scrutiny test).

335. Piety, *The Incoherence of Sorrell*, *supra* note 238, at 6; Bernstein & Lee, *Where the Consumer is the Commodity*, *supra* note 2, at 53.

336. "Detailers" is defined *supra*, at note 200.

required, as opposed to the intermediate scrutiny that commercial speech regulation typically receives.[337] Justice Breyer dissented from the application of heightened scrutiny because the law had only indirect and incidental burdens on speech that was "entirely commercial."[338] Several points flow from the *Sorrell* Court's analysis.

First, using categories of "disfavored" speakers and "disfavored" content as the basis for constitutional protections and standard of review determinations is doctrinally weak. Taken to its logical end, most laws affecting speech would violate the First Amendment because most laws could be characterized as disfavoring content or speakers. But, many laws survive First Amendment scrutiny even though they disfavor speakers and/or content. Defamation law, obscenity law, and the Espionage Act disfavor content, to name a just a few examples, but they are constitutional limitations on speech Testimonial privileges, such as attorney-client and doctor-patient, disfavor speakers, but they are constitutional limitations on speech. Thus, labeling content or speakers as "disfavored" does not provide much of a basis, if any, to determine whether a speech restriction violates the First Amendment or a higher standard of review is necessitated.

Moreover, several Roberts' Court decisions disfavor content and/or speakers. In *Garcetti v. Ceballos*, the Court held that a government employee does not have First Amendment rights in speech that relates to his job duties.[339] This law disfavors a class of speakers (government employees) and content (speech that relates to their job duties as public servants). In *Morse v. Frederick*, the Court held that a school could punish a student that engages in speech that could reasonably be viewed as advocating illegal drug use.[340] The *Morse* holding disfavors speakers (students) and content (speech that could reasonably be viewed as advocating illegal drug use).[341] In *Holder v. Humanitarian Law Project*, the Court disfavored speakers that sought to communicate with groups

337. The Court gives short-shrift to the intermediate scrutiny analysis required by *Central Hudson* by offering little more than the conclusory assertion that "the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied." Sorrell, 131 S. Ct. at 2668–72.

338. Sorrell 131 S. Ct. at 2685 (Breyer, J., dissenting).

339. Garcetti v. Ceballos, 547 U.S. 410 (2006).

340. Morse v. Frederick, 551 U.S. 393 (2007).

341. The sign Joseph Frederick unfurled across the street from his school as the Olympic Torch Relay Parade passed by read, "Bong Hits for Jesus." The majority acknowledged that the message was "cryptic" but was able to glean this as a message advocating the use of illegal drugs. Id. at 401. In concurrence, Justice Alito sought to emphasize the outer limits of the holding by stating that it would not apply to speech that questioned the policy of the war on drugs or the benefits of medicinal cannabis. Id. at 422 (Alito, J., conurring). Based on Alito's concurrence and the express language of the holding, presumably a student that unfurled a banner reading, "Legalize Pot. Then, Do Bong Hits for Jesus," would receive First Amendment protection.

designated as terrorist organizations, even if the content involved information regarding how to legally operate through international legal regimes.[342] In *McBurney v. Young*, the Court held that a state law prohibiting non-Virginia citizens from making use of Virginia's freedom of information act did not violate the First Amendment.[343] This is a clear case of the Court upholding a state law that disfavors a group of speakers—non-Virginians.

In addition to the doctrinal flimsiness of "disfavored" speakers and content as a basis for First Amendment determinations, the Court's application of these categories to describe pharmaceutical corporations would be "risible," if it were not so disheartening.[344] The Court applied these categories in *Citizens United* as well.[345] Ironically, the Court's use of "disfavored" speakers as a classification with First Amendment significance originated in civil-rights era case law.[346] These speakers were deemed worthy of First Amendment protection because of the struggles they faced in having a voice in the democratic process. Applying the "disfavored speaker" concept to multi-billion dollar for-profit companies seeking physicians' prescribing histories to boost sales tarnishes the historical context of "disfavored" speakers in Supreme Court jurisprudence and defies reality.[347] In terms of having the ability to voice a message, pharmaceutical companies are far from disfavored or disadvantaged. One need only watch a few minutes of television before an advertisement for some drug will appear.

Another questionable aspect of *Sorrell* is the Court's statement that the Vermont law prevents detailers and pharmaceutical companies from

---

342. Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

343. McBurney v. Young, 133 S. Ct. 1709 (2013).

344. See PIETY, BRANDISHING THE FIRST AMENDMENT, *supra* note 250, at 50 ("To cast [major commercial advertisers] as 'disadvantaged' or lacking an adequate opportunity for a 'voice' is risible."); *see also*, Western Tradition P'ship, Inc. v. Attorney General of State, 271 P.3d 1, 19 (2011) (Nelson, J., dissenting) ("the notion that corporations are disadvantaged in the political realm is unbelievable."), *rev'd*, American Tradition P'ship, Inc. v. Bullock, 132 S.Ct. 2490 (2012).

345. Citizens United, 558 U.S. at 340.

346. *See also*, Piety, *The Incoherence of Sorrell*, *supra* note 238, at 5 & n. 17, 15, 26–28, 54 (2012).

347. A similar sentiment was expressed by the dissenting Montana Supreme Court Justice in a case analyzing the impact of *Citizens United* on a Montana state campaign finance law:

> [I]t defies reality to suggest that millions of dollars in slick television and Internet ads—put out by entities whose purpose and expertise, in the first place, is to persuade people to buy what's being sold—carry the same weight as the fliers of citizen candidates and the letters to the editor of John and Mary Public. It is utter nonsense to think that ordinary citizens or candidates can spend enough to place their experience, wisdom, and views before the voters and keep pace with the virtually unlimited spending capability of corporations to place corporate views before the electorate.

Western Trade Partnership, 271 P.3d at 34–35 (Nelson, J., dissenting).

communicating with physicians in an "effective and informative manner."[348] There is no constitutional right to communicate in the most effective manner.[349]

Although the Court has eroded the ability of the commercial speech doctrine to uphold regulations of commercial speech, it has not been eviscerated. Justice Thomas believes that *Central Hudson* should not apply when government regulation seeks to keep the public "ignorant in order to manipulate their choices in the marketplace."[350] An opt-in regime does not seek keep the public ignorant to manipulate their market experience. To the contrary, it seeks to facilitate the disclosure of information by commercial actors regarding their data processing practices so that individuals may make informed choices about whether to consent to data processing. Thus, a common objection by those seeking to limit the scope of the commercial speech doctrine is not applicable to an opt-in requirement.

D. Erosion and Inversion of Other First Amendment Law

The Court's erosion of the commercial speech doctrine is not unique and is the result of a decades-long movement to use the First Amendment as source of law to protect economic interests.[351] The Court is using the First Amendment as a sword to strike down other regulations intended to serve the public interest, such as in *Citizens United* where the Court held that a limitation on campaign finance regulations violated the First Amendment rights of corporations and unions.[352] Also, the Court's inversion of the commercial doctrine is not the only example of the Roberts' Court turning an established First Amendment rationale on its head. The rationale for indecency regulation is another example.

---

348. Sorrell, 131 S. Ct. at 2663.

349. *See*, San Antonio Independent School Dist. v. Rodriguez, 411 U.S. 1, 36 (1973) ("[W]e have never presumed to possess either the ability or the authority to guarantee to the citizenry the most effective speech or the most informed electoral choice.").

350. 44 Liquormart, 517 U.S. at 518 (Thomas, J., dissenting).

351. *See generally,* Edwards, *The Corporate "Free Speech" Racket*, *supra* note 296; *and,* Wu, *The Right to Evade Regulation*, *supra* note 233.

352. *E.g.*, Linda Greenhouse, Harvard Commencement 2013 ("I watch with alarm as an activist Court invokes its rigidly formalistic version of the First Amendment not as shield against government suppression of speech but as a regulatory sword." (written copy: http://harvardmagazine.com/sites/default/files/PBK-oration-Greenhouse.pdf) (video: http://www.youtube.com/watch?v=VwOipR9TVZY); Purdy, *Roberts Court v. America*, *supra* note 223; Wu, *The Right to Evade Regulation*, *supra* note 233 ; *but see*, Rich Samp, *In Attack on Commercial Speech, Law Professor Sadly Supports Selective Rights*, FORBES, June 11, 2013, http://www.forbes.com/sites/wlf/2013/06/11/in-attack-on-commercial-speech-law-professor-sadly-supports-selective-rights/2/.

In 1978, the Court upheld the constitutionality of indecency regulation on broadcast radio and television, even though indecent content generally receives First Amendment protection.[353] The dual rationale of the Court was that broadcast radio and television were uniquely pervasive in society and uniquely accessible to children.[354] Thirty-one years later, indecency regulation was before the Court again.[355] Although the Court did not decide the First Amendment issue, it did offer brief dicta on the continuing viability of the dual rationale for allowing regulation of indecent content on broadcast radio and television. "The Commission could reasonably conclude that the pervasiveness of foul language, and the coarsening of public entertainment in other media such as cable, justify more stringent regulation of broadcast programs so as to give conscientious parents a relatively safe haven for their children."[356] In other words, the Court turned the rationale of *Pacifica* on its head by making the pervasiveness of other media platforms in society a reason to allow indecency rules to regulate broadcast radio and television even though they are no longer uniquely accessible and pervasive media platforms in the twenty-first century.

In addition to turning rationales upside down, the Court has also turned them backwards. Campaign finance regulation provides an example. Although much has been said and written about *Citizens United v. Federal Elections Commission*,[357] the major damage to campaign finance regulation was already done by *Federal Elections Commission v. Wisconsin Right to Life (WRTL)*, three years prior.[358] Citizens United was the proverbial nail in the coffin. Prior to the 2002 Bipartisan Campaign Reform Act (BCRA), one could escape the classification of "electioneering communication" by avoiding magic words, like "vote for" or "vote against." This avoidance was easily accomplished because one could make an ad seemingly focused on an issue, but clearly implying or associating a candidate with that issue. One purpose of BCRA was to avoid this circumvention of the electioneering law by prohibiting not only the express advocacy for or

353. Federal Commc'n Comm'n v. Pacifica Found., 438 U.S. 726 (1978).

354. Id. 748–49.

355. Federal Commc'n Comm'n v. Fox Television Stations, Inc., 556 U.S. 502 (2009) ("Fox I"). The Court reheard this case in 2012. 567 U.S. –, 132 S. Ct. 2307 (2012). In both instances, the Court did not address the First Amendment issue. In 2009, it held that the FCC did not violate the Administrative Procedures Acts by reversing its decades-long policy and declaring that "fleeting expletives" could now be considered indecent. In 2012, the Court held that the rule change violated the due process rights of the respondents because of lack of notice of the change.

356. Fox I, 556 U.S. at 529–30.

357. Citizens United v. Federal Election Comm'n, 558 U.S. 310 (2010).

358. Federal Elections Comm'n Wisconsin Right to Life, 551 U.S. 449 (2007) ("WRTL").

against a candidate, but also the functional equivalent of express advocacy. In *WRTL*, the Court essentially reinstituted the magic words test and thereby removed the teeth of the law.[359] The Court held that an ad was not subject to regulation as an "electioneering communication" if it had at least one reasonable interpretation other than express advocacy for or against a candidate. This rationale turned the law backwards.

Not only did the *WRTL* holding turn the law backwards, it raised questions about the Roberts' Court consistency in how it treats speakers and content. The *WRTL* Court stated, "Where the First Amendment is involved, the tie goes to the speaker, not the censor."[360] But, the same day that the Court issued *WRTL*, it issued *Morse v. Frederick* where the tie did not go to the speaker, even though the message had more than one reasonable interpretation. In *WRTL*, even if an ad could reasonably be interpreted as express advocacy or its functional equivalent, it was not considered an "electioneering communication" so long as it had at least one other reasonable meaning. In *Morse*, so long as one reasonable interpretation of a speech was the advocacy of illegal drug use, then it did not matter if the speech had other reasonable, permissible interpretations. The speech could be prohibited without violating the First Amendment. In *Morse*, the tie went to the censor.

One could reasonably distinguish *WRTL* and *Morse* by noting that one involved student speech and the other did not. That distinction, however reasonable, is not the only defensible interpretation of the Roberts Court's approach to free speech rights. Erwin Chemerinsky observed that the Roberts' Court is "Not a Free Speech Court."[361] Despite the Roberts Court's invocation of the related concepts that "more speech, not less, is the governing rule"[362] and that the real solution to harmful speech is more speech,[363] several decisions evince a lack of commitment to these principles.[364] While acknowledging that

359. WRTL, 551 U.S. at 531 (Souter, J., dissenting).

360. WRTL, 551 U.S. at 474.

361. Erwin Chemerinsky, *Not a Free Speech Court*, 53 ARIZ L. REV. 723 (2011); *see also*, Fisk & Chemerinsky, *Unequal Treatment?*, *infra* note 373, (noting the Court's disparate treatment between union and corporate speech in the context of campaign finance regulation, as well as the limited speech rights afforded to government employees versus the robust protection provided to a non-member of public-sector union).

362. Citizens United, 558 U.S. at 361.

363. *See*, United States v. Alvarez, 132 S. Ct. 2537, 2550 (2012).

364. In illustrating that the Roberts Court is not a free speech court, Chemerinsky cites several cases that result in less speech. *Garcetti v. Ceballos* results in less government employee speech because the Court held that a government employee does not have First Amendment rights when speaking in his official capacity. *Id.* at 726. *Morse v. Frederick* results in less speech because it prohibits speech that could reasonably be interpreted as advocating illegal drug use, even if it could be reasonably interpreted as conveying something else, including a "silly and incoherent" message. *Id.* at 728. *Beard v. Banks* results in less speech because it allows prisons to withhold from some prisioners access to all newspapers, magazines, and photographs. *Id. Holder v. Humanitarian Law Project* results in less

the Roberts' Court is not wholly opposed to free speech rights, Chemerinsky concluded that an analysis of several free speech cases "reflects the conservative majority's hostility to campaign finance regulations, rather than a pro-speech commitment."[365] Lyrissa Barnett Lidsky engaged a related question: is the Roberts Court "Not a Free Press Court?"[366] Her answer was equivocal, although ultimately a gloomy one for those who value the role of the Fourth Estate in our constitutional structure.[367] Finally, a recent empirical study analyzing decisions from 1946 through 2011 found that the current Court has been the most favorable to business during that time period.[368]

In conclusion, a faithful application of the *Central Hudson* test should result in a finding that at opt-in regime is constitutionally permissible under the First Amendment. The government has substantial interests in protecting the privacy of individuals, preventing overreaching of data processors, and avoiding the commodification of natural persons. The commercial speech doctrine and its rationale favor expanding consumer choice, not in restricting it. An opt-in regime directly and materially advances each of these interests because it ensures that online commercial actors cannot process data without first receiving affirmative, express, and informed consent. Finally, an opt-in regime is narrowly tailored to serves these interests. An opt-out regime in which individuals are unaware of how their personal data is used and traded in online markets is insufficient because it is not as effective as an opt-in regime in advancing these state interests.[369]

Although a faithful application of the *Central Hudson* test should result in finding an opt-in requirement constitutionally permissible, the Court's erosion and inversion of the commercial speech doctrine suggest

---

speech because it prohibits communication with entities designated as "foreign terrorist organizations," even if the speech provides guidance on how to use international law to peacefully resolve disputes. *Id.* at 728–29. Another case that counters the notion that the Roberts Court is a free speech court is *Hollingsworth v. Perry*, 558 U.S. 183 (2010). In a 5–4 per curiam opinion, the Court held that the Proposition 8 bench trial could not be transmitted to five other federal courts via a closed-circuit feed. The Court based its decision on a purported procedural flaw by the district court in amending its local rules. Justice Breyer's dissent notes that the Court rarely, if ever, intervenes in matters of administration of lower court procedures. Id. at 203, (Breyer, J., dissenting).

365. Chemerinsky, *Not a Free Speech Court*, *supra* note 361, at 724.

366. Lyrissa Barnett Lidsky, *Not a Free Press Court?*, 2012 B.Y.U. L. REV. 1819 (2012).

367. Lidsky stated that the Roberts Court is a free press court in the sense that it protects unpopular speech, limits medium-specific distinctions for First Amendment purposes, and broadly defines speech of public concern. *Id.* at 1821. But, the Roberts Court is not a free press court in that it "appears to see the 'Fourth Estate' as little more than a self-serving slogan bandied about by media corporations." *Id.* In light of this conclusion, Lidsky takes solace in the paucity of free press cases adjudicated by the Roberts Court. *Id.*

368. Lee Epstein, William M. Landes, & Richard A. Posner, *How Business Fares in the Supreme Court*, 97 MINN. L. REV. 1431 (2013).

369. *See generally,* Sovern, *Opting In, Opting Out*, *supra* note 44.

that a current majority of the Court may not uphold legislation imposing an opt-in requirement. More likely, the Roberts Court will continue to expand protection for commercial speech.[370] There is, however, another First Amendment analysis that may sustain an opt-in regime as constitutionally permissible, perhaps even constitutionally required. This analysis flows from an analogy regarding the First Amendment rights of non-members of public-sector unions.

E. A First Amendment Opt-In Requirement

In recent years, the Supreme Court has decided two cases involving an opt-in requirement, *Davenport v. Washington Education Association*[371] and *Knox v. Service Employees International Union*.[372] Both cases involve fees charged to non-members of public-sector labor unions and include First Amendment analysis.[373] *Davenport* involves analysis of state legislation that imposed an opt-in requirement. *Knox* did not involve any legislation that imposed an opt-in requirement. Nonetheless, the *Knox* Court held that an opt-in approach was required as a matter of constitutional law, even though this specific issue was not briefed or argued by the parties.[374] These cases provide some guidance as to how the Court might analyze a claim that an opt-in requirement prior to data processing violates a data processor's First Amendment rights. Specifically, these cases may be helpful in establishing that legislation requiring an online commercial data processor to receive an individual's opt-in consent prior to data processing would be at least constitutionally permissible under the First Amendment.

---

370. PIETY, BRANDISHING THE FIRST AMENDMENT, *supra* note 250, at 223 ("[T]he rhetoric in [*IMS Health* and *Citizens United*] suggests that increased protection for commercial speech is almost inevitable.").

371. 551 U.S. 177 (2007).

372. 132 S. Ct. 2277 (2012).

373. At the time of writing this Article, a third case involving the First Amendment rights of non-members of public-sector unions was pending before the Court, *Harris v. Quinn*, 656 F.3d 692 (7th Cir. 2011), *cert. granted*, 134 S. Ct. 48 (2013). In *Harris*, the Seventh Circuit held that it does not violate the First Amendment rights of non-members of public-sector unions when a state statute requires that they pay fees to "support legitimate, non-ideological, union activities germane to collective-bargaining representation." *Id.* at 693–94, 697. "In colloquial terms, the petitioners in *Harris* seek to have the Supreme Court declare that, as a matter of the First Amendment, all government employment must be on a 'right-to-work' basis." Catherine Fisk & Erwin Chemerinsky, *Unequal Treatment? The Speech and Association Rights of Employees: Implications of* Knox and *Harris*, Am. Cons. Soc'y Issue Br. (Feb. 2014) (*citing* Transcript or Oral Argument at 21, Harris v. Quinn, __ S. Ct. __ (2014) (No. 11-681)). The Court ruled in favor of the petitioners holding that the First Amendment does not permit "a State to compel personal care providers to subsidize speech on matters of public concern by a union that they do not wish to join or support." Harris v. Quinn, 134 S. Ct. 2618 (2014).

374. Knox, 132 S. Ct. at 2298 (Sotomayor, J., concurring in the judgment); *id.* at 2306 (Breyer, J., dissenting).

Government employees are not required to join a union. Even if a government employee chooses to not join a union, many states allow the union to collect a fair share fee, also known as an agency shop fee. Because of First Amendment concerns that arise, at least in the public-sector context, these fees cannot be used for "ideological purposes that are not germane to the union's collective-bargaining duties."[375] Money spent on ideological purposes that are not germane to a union's collective bargaining duties is non-chargeable to objecting non-member employees.

In *Teachers v. Hudson*,[376] the Court established procedures to ensure that objecting non-members have the ability to effectuate this protection. This has become known as the "*Hudson* notice" requirement. Upon receiving a *Hudson* notice, a non-member employee has a set period of time to opt-out of paying the non-chargeable portion of union fees. *Hudson* did not hold, however, that the First Amendment requires affirmative consent before using a non-member employee's fees for non-chargeable expenses.[377] But, *Hudson* did not preclude an opt-in approach either. The Court considered the constitutional permissibility of an opt-in requirement in *Davenport*, which involved a Washington state law.

Washington state passed legislation requiring a union to receive a non-member employee's opt-in consent before using that non-member's fees for non-chargeable purposes. This type of law is known as "paycheck protection" legislation and other states have enacted similar laws.[378] Washington's law requires that a labor organization not use fair share fees to "influence an election or to operate a political committee, unless affirmatively authorized by the individual."[379] After being sued by a non-member employee for violating this opt-in legislation, the public school union claimed that the opt-in requirement violated the union's First Amendment rights. In a divided en banc opinion, the Washington Supreme Court agreed with the union, reasoning that heightened scrutiny was required and not satisfied because the opt-in law deviated from the balance between non-members' and the union's First Amendment rights as established by United States Supreme Court precedence.[380] The Court, however, disagreed.

---

375. Davenport, 551 U.S. at 181 (*citing* Abood v. Detroit Bd. of Ed., 431 U.S. 209, 235–36 (1977)).

376. 475 U.S. 292 (1986).

377. Davenport, 551 U.S. at 181.

378. Ciarra Torress-Spelliscy, *Taking Opt-In Rights Seriously: What Knox v. SEIU Could Mean for Post-Citizens United Shareholder Rights*, 74 MONT. L. REV. 101, n. 47 (2013) (collecting statutes).

379. Wash. Rev. Code § 42.17.760 (2006).

380. State ex. Rel. Washington State Public Disclosure Comm'n v. Washington Ed. Assn.. 156 Wash.2d 543 (2006) (en banc). In the past, the Court has recognized that the First Amendment rights of

In *Davenport*, the Court held that Washington's legislatively imposed opt-in requirement was constitutionally permissible.[381] The Court expressly limited the scope of its decision to the "unique context" of public sector-unions.[382] In dicta, the Court noted that application of an opt-in law in the private-sector union context "presents a somewhat different constitutional question" because the fees are collected through "contractually required action taken by private employers rather than by government agencies."[383] The Court tempered its dicta by noting that it was "not suggest[ing] that the answer must be different."[384] While *Davenport* held that legislation imposing an opt-in requirement in the public-sector union context was constitutionally permissible, *Knox* went much further.[385]

Knox arose under California law, which does not have an opt-in law (aka "paycheck protection" legislation) similar to the Washington law in *Davenport*. Sometime after a public-sector union issued its annual *Hudson* notice, it imposed a temporary special assessment on employees, including non-members, to fight a ballot measure seeking to establish paycheck protection legislation in California. Non-members filed a class action against the union alleging it violated their First Amendment rights by imposing the special assessment without providing a new *Hudson* notice and opportunity to opt-out.

The *Knox* Court held that not only must a public-sector union provide a new *Hudson* notice before imposing a special assessment or dues increase, the First Amendment requires the union to receive a non-member's affirmative consent before exacting funds from that employee.[386] In dissent, Justice Breyer described the Court's holding as "mandat[ing] an 'opt-in' system in respect to the payment of special

---

unions must be balanced with the First Amendment rights of non-members. *E.g.*, International Ass'n of Machinists v. S.B. Street, 367 U.S. 740 (1961). "The Court's focus on protecting the speech rights of the union, however, vanished in subsequent cases." Fisk & Chemerinsky, *Unequal Treatment?*, *supra* note 373, at 3.

381. Davenport, 551 U.S. at 191.

382. Id. at 190.

383. Id.

384. Id.. at 190, n. 4.

385. One commentator noted that "[t]he *Knox* holding represents a titanic shift by placing corporate managers and union leaders in decidedly divergent legal positions." Torres-Spelliscy, *Taking Opt-In Rights Seriously*, *supra* note 378, at 104–05. Torres-Spelliscy explains that *Citizens United* allows corporations to ignore dissenting shareholders views in making political expenditures whereas *Knox* prevents unions from making similar expenditures without receiving affirmative consent from non-member employees and that this divergence is problematic as matter of basic equity and fairness. *See generally*, id.; *see also*, Fisk and Chemerinsky, *Unequal Treatment*, *supra* note 373, at 10 ("The [*Citizens United*] Court was untroubled by the fact that spending from general corporate revenues meant that the corporation was spending the shareholders' money on political activities without their consent and even against their political views.").

386. Knox, 132 S. Ct. at 2296.

assessments."[387] In separate opinions, both Justices Sotomayor and Breyer expressed concern that the majority's constitutionally required opt-in holding decided a constitutional issue that neither party briefed or argued.[388]

While *Davenport* and *Knox* involve First Amendment analysis of an opt-in requirement in the context of the relationship between a non-member employee and a public-sector union, there are lessons from these cases that apply in the context of a relationship between an individual and an online commercial data processor. First, the *Knox* Court reasoned that an opt-in approach was constitutionally required because defaults should represent the probable preferences of most individuals affected.[389] Several studies show that the preference of most consumers is that they not be subject to online behavioral advertising.[390] One critique of these studies is that the actions of individuals do not align with their responses in the studies and, therefore, this means that the studies are flawed. Individuals are willing to trade their privacy for the benefits of online data processing, such as free email, social networking, and useful search engines. In other words, individuals "pay" for these services with their data and the concomitant loss of privacy.

Strandburg, however, make a persuasive argument that this market perspective is flawed. Individuals do not know the prices they are paying for these services because the costs are intentionally hidden from individuals by the firms that process the data[391] and because not all costs are known at the point of purchase. Indeed, some costs occur after the transaction when the data is used for new purposes, including purposes that could not be known at the point of purchase because they did not exist at that time. In a data processing world, both costs to individuals and the economic value to data processors are intentionally hidden,

387. Id. at 2306 (Breyer, J., dissenting).

388. Id. at 2298 (Sotomayor, J., concurring in the judgment); id. at 2306 (Breyer, J., dissenting).

389. Knox, 132 S. Ct. at 2290.

390. *E.g.*, Joseph Turow, et al., *Americans Reject Tailored Advertising & Three Activities that Enable It*, Sept. 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214; Aleecia McDonald and Lorrie F. Cranor, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising* (TPRC 2010 Aug 2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092##.

391. Strandburg identified three types of information that individuals lack access to, but need to make an informed decision regarding whether to allow data processing: (1) types of harms, prevalence of those harms, and their costs; (2) the firm's collection, storage, and use practices; and (3) how the recently collected information is connected with previously collected data available to the firm and how the recently collected information may be disclosed to integrated companies or third-parties. Strandburg, *Free Fall*, *supra* note 24, at 44–45. Others have made substantially similar points. *E.g.* TUROW, DAILY YOU, *supra* note 4, at 8 ("Part of the reason for the lack of action may be that neither citizens nor politicians recognize how deeply embedded in American live these privacy-breaching and social-profiling activities are.").

leaving consumers ignorant. Quite simply, without adequate information, the market does not function in reality as the theory requires. Thus, an opt-in requirement in the online data processing context is at least constitutionally permissible, because as in *Knox*, such a requirement represents the probable preference of most individuals.

Second, *Davenport* and *Knox* both involve a state actor. The *Davenport* Court expressly limited its holding to the "unique context" of an employee working for the government.[392] It is possible that the Court could distinguish these cases from legislation mandating an opt-in requirement between an individual and a private data processor. But, *Davenport* dicta noted that it was not suggesting that the answer must be different in the context of a non-member employee and a private-sector union. Moreover, *Knox* provides reasoning that suggests the public-private dichotomy is not controlling in analyzing the constitutionality of a law requiring opt-in consent.

The *Knox* Court stated: "The general rule—individuals should not be compelled to subsidize private groups or private speech—should prevail."[393] In reference to this statement, Ciarra Torres-Spelliscy wrote: "Another way of framing this is the Supreme Court hereby privileged the autonomy of the individual over the autonomy of the labor organization to speak (or not speak) politically."[394] In other words, the Court found that the interest of the individual employee took preference over the interest of the union. Following this logic, an opt-in approach is at least constitutionally permissible in the data processing context because the interest of the individual should take precedence over the interest data processors. The general rule should prevail: Individuals should not be compelled to subsidize the private speech of for-profit commercial actors by allowing unconsented data processing.

The *Knox* Court also stated that "[c]ourts 'do not presume acquiescence in the loss of fundamental rights.'"[395] At least some privacy rights are fundamental.[396] Whether informational privacy is a fundamental right is not established, but in a recent case involving legislation regulating data access, the Court described privacy as a concept that is "integral to the person" and "essential to freedom."[397]

---

392. Davenport, 551 U.S. at 190.

393. Knox, 132 S. Ct. at 2295.

394. Torres-Spelliscy, *Taking Opt-In Rights Seriously*, *supra* note 378, at 114.

395. Knox, 132 S. Ct. at 2290 (*quoting* College Savings Bank v. Florida Prepaid Post Secondary Ed. Expense Bd., 527 U.S. 666 (1999)).

396. *See e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965).

397. Sorrell, 131 S. Ct. at 2672. The full sentence in *Sorrell* is: "Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers." *Id.* A legislatively imposed opt-in requirement would not be the government manipulating the concept of privacy to support ideas it prefers. Rather, it would be the government

Thus, the absence of a state actor should not preclude reliance on the opt-in analysis in *Knox* and *Davenport* when analyzing an opt-in requirement in the online commercial data processing context because the privacy rights and interests of individuals are at risk, interests that are integral to the person and essential to freedom.

Third, the *Knox* Court noted that closer legal analysis of opt-in versus opt-out regimes is overdue.[398] It stated that very little attention has been paid to this design choice and that most decisions regarding opt-in versus opt-out are the result of historical accident, rather than reasoned analysis.[399] Online data processing by commercial actors is an area where closer legal analysis of opt-in versus opt-out regimes is warranted because of the lack of choice individuals currently have in being subject to data processing and the growing ubiquity of the data processing industry that affects individuals' lives and society.[400]

Fourth, the *Knox* Court noted that the opt-out approach was a "remarkable boon" for unions.[401] The opt-out approach (if there is any option at all) has been a remarkable boon for commercial data processors because individuals have little information and little, if any, choice when it comes to making an informed decision about allowing a private company to process their data. Relatedly, the *Davernport* Court described the Washington's legislatively imposed opt-in requirement as a "modest limitation" on an "extraordinary benefit."[402] Requiring online

---

seeking to allow individuals to make informed choices about what data they share with online commercial data processors. As the next paragraph above shows, the probable preference of most individuals is to have a choice in what data they share and how it is used.

398. Knox, 132 S. Ct. at 2290.

399. Id.

400. A closer analysis of opt-in versus opt-out regimes is warranted in contexts outside of the First Amendment as well, including the Fifth Amendment. Although the Court did not use the phrase "opt-in," that term aptly describes the Court's requirement that one must expressly invoke the right to silence before the Fifth Amendment right against self-incrimination applies. Salinas v. Texas, 570 U.S. –, 133 S. Ct. 2174 (2013). Leaving aside the irony that one must affirmatively invoke the right to remain silent, *Salinas* provides persuasive authority for the constitutionality of an opt-in regime in the context of online data processing by commercial actors. The right against self-incrimination is expressly set forth in the U.S. Constitution. U.S. CONST. AMEND. V. ("No person . . . shall be compelled in any criminal case to be a witness against himself . . ."). Yet, the Court decided that one must expressly invoke this right before he can be afforded its protections.

If one must opt-in before the constitutional right against self-incrimination applies, then it seems eminently reasonable to find an opt-in requirement at least constitutionally permissible in the context of online commercial data processing. The right against self-incrimination protects the liberty interests threatened by a criminal conviction, including physical imprisonment. The right to be free from unwanted data processing is surely a lesser interest, but a liberty interest nonetheless. If a constitutional right that protects against infringements of physical liberty requires an opt-in process, an opt-in requirement protecting against infringements by online commercial data processors should comfortably fall within the scope of constitutionally permissible opt-in requirements.

401. Knox, 132 S. Ct. at 2290.

402. Davenport, 551 U.S. at 2378.

commercial data processors to receive an individual's opt-in consent prior to data processing is a modest limitation on the extraordinary financial and informational benefits that these actors receive from the aggregation of data.

If an opt-in approach is constitutionally required when a public-sector union seeks to impose a special assessment or a dues increase upon a non-member employee, an opt-in approach is at least constitutionally permissible in the context of online, for-profit data processing, if not constitutionally required.[403]

VI. CONCLUSION

The preface to a popular Contracts Law casebook states: "No study of law is adequate if it loses sight of the fact that law operates first and last, *for*, *upon*, and *through* individual human beings."[404] Both private corporations and public government are instrumental legal fictions designed to serve humankind, these entities are not ends in themselves.[405] Unfortunately, the law has lost sight of the interests of individual human beings in the online data processing context because there has been an overemphasis on the rights and freedoms of data processors and an undervaluing of the rights and freedoms of individuals.[406] This overemphasis flows from the economic interests of commercial actors and the Court's increasing willingness to substitute its judgment for that of legislative bodies.

In the commercial speech context, Justice Rehnquist's dissent in *Virginia Pharmacy* alluded to *Lochner v. New York*[407] in warning that the majority's use of the First Amendment was reminiscent of the discarded jurisprudence where the Court invoked the Due Process clause to override the social and economic judgments of legislative bodies.[408] In his *Central Hudson* dissent, Rehnquist expressly stated the Court has

403. This Article focuses on the more modest inquiry regarding the constitutional permissibility of an opt-in regime before online commercial actors engage in data processing, as opposed to the bolder claim that an opt-in regime is constitutionally required. *Knox* opens the door to the latter proposition, but that analysis is beyond the scope of this Article.

404. CHARLES L. KNAPP, NATHAN M. CRYSTAL, HARRY G. PRINCE, PROBLEMS IN CONTRACT LAW: CASES & MATERIALS xxiii (7th ed. 2012) (emphasis in original).

405. C. Edwin Baker, *Paternalism, Politics, and Citizen Freedom: The Commercial Speech Quandary in* Nike, 54 CASE W. RES. L. REV. 1161, 1163 (2004).

406. See, Cohen, *Examined Lives*, *supra* note 6, at 1423. ("[D]ata privacy discourse has been driven by concerns for the autonomy of those who would objectify individuals—with the rights of the data processor as owner, trader, vendor, speaker, chooser. If we are serious about fostering individual freedom in reality as well as in rhetoric, this is an odd result.").

407. 198 U.S. 45 (1905).

408. Virginia Pharmacy, 424 U.S. at 784 (Rehnquist, J., dissenting) (*quoting* Ferguson v. Skrupa, 372 U.S. 726, 730 (1963)).

"return[ed] to the bygone era of *Lochner*" by striking down economic regulations under the guise of free speech protected by First Amendment.[409] Thirty-five years after *Virginia Pharmacy*, Justice Breyer's *Sorrell* dissent echoed Justice Rehnquist's concern by noting that the *Sorrell* majority "reawakens *Lochner*'s pre-New Deal threat of substituting judicial for democratic decision-making where ordinary economic regulation is at issue."[410] Commentators also note the *Lochner*-esque nature of the Court's recent First Amendment jurisprudence.[411] Should Congress pass legislation requiring online commercial actors to receive an individual's opt-in consent prior to data processing, First Amendment challenges will follow. Despite the Court's "First Amendment *Lochnerism*,"[412] the privacy interests of individuals should not be forgotten, nor subordinated to the economic interests of artificial entities in the emerging and quickly expanding age of Big Data.

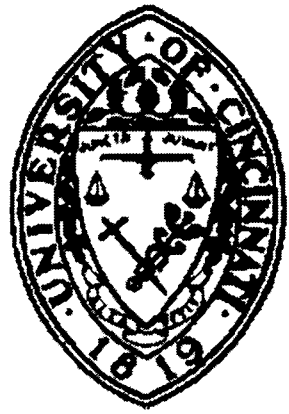
An opt-in requirement will help refocus the law on individual privacy interests, including the freedom from being commodified without consent. To the extent that data is speech subject to First Amendment protection, legislation imposing an opt-in requirement prior to data processing by commercial actors should be found constitutionally permissible under a faithful application of the commercial speech doctrine. Alternatively, the constitutionally required opt-in procedure that the Court imposed on public-sector unions in *Knox v. SEIU* should be extended to individuals in the online privacy context, at least finding that a legislatively imposed opt-in requirement is constitutionally permissible. An opt-in requirement does not solve all of the privacy concerns raised by online data processing. But, an opt-in requirement is an important part of the solution to the new privacy challenges arising in the Big Data era because it helps us regain sight that law operates first and last, for, upon, and through individual human beings.

409. Cent. Hudson, 447 U.S. at 589–91.

410. Sorrell, 131 S.Ct at 2685 (citing Cent. Hudson, 447 U.S. at 589 (Rehnquist, J., dissenting).

411. *E..g.*, Edwards, *The Corporate "Free Speech" Racket*, *supra* note 296; *and* Purdy, *The Roberts Court v. America*, *supra* note 223, at 47. *See also*, Jed Rubenfield, *The First Amendment's Purpose*, 53 STAN. L. REV. 767, 771 (2001) (comparing *Lochner* and *United States v. O'Brien*, 391 U.S. 367 (1968)).

412. The Northern Kentucky Law Review published a symposium issue with various perspectives on what "First Amendment *Lochnerism*" means. *See generally*, 33 N. KY. L. REV. 365 (2006).


UNIVERSITY OF CINCINNATI
1819