WITH BIG DATA SHOULD COME BIG RESPONSIBILITY: REGULATING SUPPLY AND DEMAND OF ALTERNATIVE DATA

*Abbe Dembowitz**

INTRODUCTION

For centuries, Americans have enjoyed the right to privacy—the "right to be let alone."[1] The privacy interests of Americans, however, face a unique threat in the form of a "Data Rush"—the Gold Rush of the 21st Century.[2] Through a strategy known as "alternative data" investment, the biggest hedge fund managers across the world are purchasing, collecting, and trading on a seemingly boundless amount of personal information—a practice that is almost entirely unregulated. These funds, in the name of innovation, are exploiting massive amounts of information that consumers generate merely by engaging in their day-to-day activities like walking, shopping, and eating. Current insider trading laws enable funds to escape liability through contractual sign-off provisions that impose no fiduciary duty on either the companies gathering the data or the funds purchasing it. This contribution first discusses the current landscape of alternative data. It then proposes a legislative imposition of explicit informed consent requirements on companies that sell customer information. In light of the pervasiveness of the alternative data practice, the proposed legislation would explicitly deem any person in possession of the confidential information a fiduciary. Companies that sell the private consumer information without consent would thus violate their fiduciary duty owed to consumers. Consequently, fund managers who fail to do their due diligence and trade on such information would now be subject to insider trading prosecution under a misappropriation theory. This proposition aims to empower consumers without stifling innovative investment techniques. Although technological advancements open the door for privacy infringements, they also present an opportunity for new and innovative legislation.

---

* Abbe Dembowitz is a *juris doctor* candidate at the Georgetown University Law Center, with expected graduation in 2020. She is a Featured Online Contributor for Volume 56 of the *American Criminal Law Review*.

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

2. *See* Kara M. Stein, Commissioner, SEC, Georgia State University College of Law – Henry J. Miller Distinguished Lecture Series: From the Data Rush to the Data Wars: A Data Revolution in Financial Markets (Sept. 27, 2018).

I. BACKGROUND

The definition of "alternative data" is rather amorphous; it shifts with every technological development. Sources of alternative data presently include sensors from internet-connected machines or "smart" devices, pharmacological prescription data, e-commerce receipts and credit-card transaction data, and retail brick and mortar activity (e.g., satellite drones analyzing parking-lot traffic).[3] An additional source of alternative data consists of the information that web services and mobile apps receive from users (e.g., Foursquare geolocations and foot traffic), as well as social media and social sentiment data, geolocation information, and online pricing and inventory data.[4] In effect, every step you take, every swipe of your credit card, is watched, packaged, and traded on. This contribution focuses specifically on the use of private consumer data.

According to Ernst and Young's 2017 Global Hedge Fund and Investor Survey, 78% of hedge funds reported that they currently use or expect to use alternative data, an increase from the reported figure of roughly 50% in 2016.[5] Additionally, 80% of those surveyed anticipate that this "non-traditional data" will be "critical" to their businesses within the next five years.[6] This data has become so valuable that top firms like Point72 Asset Management LLP and Tiger Global Management LLC have paid more than $2 million each for an annual subscription to Yodlee Inc.[7] Although its main business is to provide online personal-finance tools to large banks, in 2014, Yodlee made a whopping 10% of its total revenue from alternative data sales alone.[8] But as businesses increase their net revenues, consumers lose their privacy rights.

---

3. Jeffrey D. Neuburger, et. al., *Big Data and Hedge Funds; An Emerging Trend with its Own Legal and Compliance Issue*, PROSKAUER ROSE (July 2017), https://www.wellsfargo.com/com/securities/markets/equity-sales/prime-services/publications/update-07-17/#data. Sources also include, but are not limited to, meteorological and agricultural data; energy supplies and usage; and shipping/freight activity.

4. *Id.*

5. *See* Peter I. Altman, Kelly Handschumacher & Jennifer Hustwitt, *Big Data and the Risks of Insider Trading*, 50 SEC. REG. L. REP. 426, 426 (Mar. 19, 2018), https://www.akingump.com/images/content/6/5/v2/65585/spBigData-SRLR-March-19-2.pdf.

6. *Id.*

7. *See* Bradley Hope, *Envestnet Deal Values Yodlee at $590 Million: Deal Merges Provider of Online Investment Tools with Financial-App Maker*, WALL STREET JOURNAL (Aug. 10, 2015), https://www.wsj.com/articles/envestnet-deal-values-yodlee-at-590-million-1439245934. Yodlee was acquired by Envestnet Inc. in 2015.

8. *See* Bradley Hope, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors*, WALL STREET JOURNAL (Aug. 6, 2015), https://www.wsj.com/articles/provider-of-personal-finance-tools-tracks-bank-cards-sells-data-to-investors-1438914620.

The complicated chain of data sales involves the consumer, the vendor or company who contracts with the consumer, the data broker who transforms and packages the data, and the investment managers who purchase and trade on that information.[9] In practice, that means Consumer A buys a phone from Company B. Unbeknownst to them but sandwiched into the terms of their agreement, Consumer A has agreed to let Company B sell off their cell site location, credit card information, and personal information including age, date of birth, and social security number. Company B then sells to it Data Broker C who "anonymizes" the data (a process discussed below) and sells it to Hedge Fund D. Hedge Fund D finally "sift[s] through the noise and correctly identif[ies] . . . trading signal[s] that will ultimately create alpha."[10] In response to this practice, the SEC has promised that innovative regulation is on the horizon to deter "those that threaten our markets, while at the same time [support] the innovation that drives economic growth."[11] But this solution cannot be achieved without the regulation of both demand- *and* supply-side companies.

In short, alternative data is a supply and demand market. Without demand for alternative data, supply-side consumer-facing companies would have little incentive to produce it. And without a ready supply of such data, hedge funds would likely not trade on it. As discussed, funds' increasing demand is met with increased supply of private consumer information. In order to regulate investment managers on the demand side, supply-side businesses must be required by law to obtain affirmative, informed "opt-in" consent from consumers before selling their personal data to third parties. Such legislation would not only impose a duty on businesses to not use their customers' personal information unless explicitly authorized, but would also deem any holder of that information a fiduciary. This way, not only would the companies be held accountable, but funds who trade in breach of that fiduciary duty would also be subjected to insider trading prosecution. Lawmakers must step in to

9. *See* Ian Allison, *Big Data, Big Problem: Could Wall Street See Insider Trading Lawsuits Over Selling Data Sets?*, NEWSWEEK (Oct. 11, 2017, 10:30 P.M.), https://www.newsweek.com/could-wall-street-see-first-legal-action-selling-data-sets-682188.

10. John Manning, *Hedge Funds See Huge Potential in Alternative Data*, INTERNATIONAL BANKER (Oct. 22, 2018) https://internationalbanker.com/brokerage/hedge-funds-see-huge-potential-in-alternative-data/. *See* Ian Allison, *Big Data, Big Problem: Could Wall Street See Insider Trading Lawsuits Over Selling Data Sets?*, NEWSWEEK (Oct. 11, 2017, 10:30 P.M.), https://www.newsweek.com/could-wall-street-see-first-legal-action-selling-data-sets-682188.

11. Kara M. Stein, Commissioner, SEC, Georgia State University College of Law – Henry J. Miller Distinguished Lecture Series: From the Data Rush to the Data Wars: A Data Revolution in Financial Markets (Sept. 27, 2018).

prevent companies from burying privacy right signoffs in pages of legal jargon, and hedge funds to use this information cart blanche.

II. THE SUPPLY-SIDE: COMPANIES

A. The Problem

There have been no shortage of attempts to regulate the data usage practices of supply-side companies as technology develops, none of which—at least in the US—have passed on the federal level. This article focuses on helpful pieces from the EU's General Data Protection Regulation (GDPR),[12] President Barack Obama's 2012 and 2015 proposed Consumer Privacy Bill of Rights (CPBR),[13] Senators Richard Blumenthal (D-CT) and Edward Markey (D-MA)'s proposed Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act,[14] and the Social Media Privacy and Consumer Rights Act of 2018 (SMPCRA),[15] a bipartisan bill by Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA).[16] Although all contain weaknesses, we are beyond the point of waiting for a "perfect bill" to pass legislators' desks.

Each of these bills (with the exception of the GDPR) authorizes enforcement by the Federal Trade Commission (FTC) and state attorneys general, but they vary significantly from one another in other respects. For example, the CONSENT Act requires certain providers to obtain opt-*in* consent from consumers to use "sensitive information" for data collection

12. GDPR Key Changes, EU GDPR (2018), https://eugdpr.org/the-regulation.

13. *See* Press Release, The White House Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights; WHITE & CASE LLP, WHITE HOUSE RE-INTRODUCES CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act.

14. *See* Press Release, U.S. Senate, As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights (Apr. 10, 2018), https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights.

15. Both bills are pending before the Senate Committee on Commerce, Science, and Transportation.

16. Alyson Sandler, *Senators Klobuchar and Kennedy Introduce Privacy Legislation*, COVINGTON & BURLING LLP DATA PRIVACY AND CYBERSECURITY GROUP (Apr. 25, 2018), https://www.insideprivacy.com/united-states/congress/senators-klobuchar-and-kennedy-introduce-privacy-legislation/. ("Our bill gives consumers more control over their private data, requires user agreements to be written in plain English and requires companies to notify users of privacy violations . . . .").

and tracking.[17] The SMPCRA, on the other hand, gives consumers the right to opt-*out*, allowing providers to deny services or complete access if a given user's privacy selections "creates inoperability in the online platform."[18] Where the GDPR, CPBR, and SMPCRA agree, however, is that operators must provide users with a separate text box detailing—in plain language—how the data may be used. That means no more blanket "by purchasing our [service], you hereby acknowledge, consent, and agree to the terms of this Privacy Policy" statements.[19]

Each bill responds in some form to the "Wild West" of data collection, where a simple "click here to sign your privacy rights" awaits. Social science research indicates that consumers do not understand—let alone read—lengthy privacy policies.[20] In one study, 64% of those surveyed did not know that a supermarket could sell information about what they buy to other companies.[21] Another 75% believe that when "a website has a privacy policy, it means the site will not share [their] information with other websites and companies."[22] Should legislators impose what Senator Blumenthal calls "affirmative informed consent,"[23] however, consumers will regain choice as to how their data is used and businesses can still engage in a lucrative practice. As Senators Markey and Blumenthal suggest, "[c]onsumers deserve the opportunity to opt in to services that might mine and sell their data—not find out their personal information has been exploited years later."[24]

---

17. There are two types of opt-ins: first, bundled opt-ins, where the good or service can only be bought if the consumer gives up privacy rights; and second, optional opt-ins, where the consumer can buy the good or service with or without giving up privacy. In the first scenario, all buyers will have agreed to give up private information and so there is no breach of confidentiality if a company like Verizon sells their data. Should the second opt-in be implemented, it would provide the requisite misappropriation for insider trading prosecutions discussed below.

18. *Id.*

19. Mona Ibrahim, *Why You Should Be Reading the Privacy Notices Choking Your Inbox*, POLYGON (May 28, 2018, 2:00 P.M.), https://www.polygon.com/2018/5/28/17402270/gpr-privacy-notices-privacy-policies.

20. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, COLUM. L. REV. 583, 667 (2014) (noting that consumers "are heavily influenced by the way choices are framed and harbor many preexisting assumptions that are incorrect").

21. Joseph Turow, Lauren Feldman & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, UNIV. OF PA., ANNENBERG PUB. POLICY CTR. (2005), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers;.

22. *Id*.

23. Press Release, U.S. Senate, As Facebook CEO Zuckerberg Testifies to Congress, Senators Markey and Blumenthal Introduce Privacy Bill of Rights (Apr. 10, 2018), https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights.

24. *Id.*

President Obama's initial proposal of a Consumer Privacy Bill of Rights in 2012 sought to "provide customers with more control over their data, companies with clearer ways to signal their responsible stewardship over data, and everyone with the flexibility to continue innovating in the digital age."[25] As is no surprise, big companies—specifically those in Silicon Valley—were not thrilled.[26] The main issue, however, was not that the practice would stifle innovation, but that the proposal left the onus on companies to put these privacy standards into place. Self-regulation, while perhaps sound in theory, fails to properly protect consumers. In the words of David Vladeck, former Director of the Consumer Protection Bureau of the FTC: "you have no privacy protection when the policies are written by big companies, for big companies."[27]

Senate Commerce Committee member John Thune (R-SD) recognized this issue, stating "many of my colleagues on both sides of the aisle have been willing to defer to tech companies' efforts to regulate themselves, but this may be changing."[28] As breaches become commonplace, a number of companies are increasingly open to a discussion of a basic federal privacy law. Most notably, Facebook's Mark Zuckerberg told CNN "I'm not sure we shouldn't be regulated," and Apple's Tim Cook has expressed "emphatic belief that self-regulation is no longer viable."[29] The alternative data process shows that industry players will forego consumer trust and privacy for a pretty penny on data sales. "If you want to protect consumers," Vladeck said, "you don't simply allow industry to decide what to do in a way in which they don't have any incentive to compromise."[30]

---

25. WHITE & CASE LLP, WHITE HOUSE RE-INTRODUCES CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act.

26. *See* Gary Shapiro, CEO of the Consumer Electronics Association (represents Apple, Samsung, and other device makers) felt that legislation like President Obama's proposal would "hurt American innovation and choke off potentially useful services and products."; Brendan Sasso, *Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides*, THE ATLANTIC (Feb. 27, 2015), https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

27. Interview with David Vladeck, Former Director of Consumer Protection Bureau, FTC and Georgetown University Law Center Professor, in Washington, D.C. (Oct. 31, 2018).

28. Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

29. *Id.*

30. Natasha Singer, *Why a Push for Online Privacy is Bogged Down in Washington*, N.Y. TIMES. (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

B. The Solution

In order to (a) create a duty of privacy protection between consumers and big businesses without relying on self-regulation and (b) not quash innovation, the legislature should create a set of requirements for all consumer-based services, not just online or social media companies. As suggested by prior legislative efforts, a mandatory opt-in provision should be an entirely separate and distinguishable pop-up that requests—in plain English—consent to a set of explicit possible uses, broken down into categories such as cell-site location, social security number, and credit card information. The request should be in an "intelligible and easily accessible form,"[31] with the purpose, intention, and specifics of each use plainly stated. This would include everything from geolocation to social security number to credit card information. While complete control of consumer information is no longer possible, individuals "can and should have a say in the matter."[32]

The choice to sign private personal data away must rest with the consumer. According to a 2014 Pew Research study, more than 90% of Americans felt they had lost control of their personal data.[33] Two-thirds of study respondents wanted lawmakers to step in, at least in some capacity, to regulate companies' use of their private data. Many consumers are—at the very least—willing to accept a trade-off:[34] data in exchange for access to free online services, or a cheaper TV service, to name a few.[35] To account for this, President Obama articulated seven basic principles for subsequent legislation: individual control,[36] transparency,[37] respect for the

31. GDPR Key Changes, EU GDPR (2018), https://eugdpr.org/the-regulation.
32. Ron Yokubaitis, *It's Time to Take Our Privacy Back from Tech Companies*, THE HILL (Jan. 19, 2018, 7:30 A.M.), https://thehill.com/opinion/technology/369573-its-time-to-take-our-privacy-back-from-tech-companies.
33. *See* Dan Kedmey, *9 in 10 Americans Feel They've Lost Control of Their Personal Data*, TIME (Nov. 12, 2014), http://time.com/3581166/privacy-personal-data-report/ (citing Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/).
34. *Id.* ("while many Americans are willing to share personal information in exchange for tangible benefits, they are often cautious about disclosing their information and frequently unhappy about that happens to that information once companies have collected it.")
35. *See* Stacey Higginbotham, *AT&T's GigaPower Plans Turn Privacy Into A Luxury That Few Would Choose* (May 13, 2014, 1:35 P.M.), GIGAOM, https://gigaom.com/2014/05/13/atts-gigapower-plans-turn-privacy-into-a-luxury-that-few-would-choose.
36. Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
37. Consumers have a right to easily understandable and accessible information about privacy and security practices.

context in which the data was obtained, access and accuracy,[38] focused collection,[39] security,[40] and accountability.[41] Though the bill died a slow death in Congress, the "respect for context" principle should be carried over to new legislation. It means that people "have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[42]

Danny Weitzner, co-architect of the CPBR, looked to Waze, a community-based traffic and navigation app, as an example of the limits consumer buy-in data sharing.[43] While consumers were generally willing to share location information that allowed ride-sharing and navigation apps because it enables the apps to serve their purpose, Waze ran into resistance in requiring that location settings always be on.[44] Weitzner notes the respect for context principle "would have prohibited [Cambridge Analytica] from unilaterally repurposing research data for political purposes" because it establishes a right "not to be surprised by how one's personal data [is] issued."[45] Similarly, hedge funds trading on consumers' geolocation and spending does not fall within the context associated with a cell phone purchase or swipe of a credit card.

Investment managers argue that they are "generally interested in aggregates and neither require nor want personal details held within the data."[46] While that may be true, the opportunity to uncover an individual's specific data from an "anonymized" set is larger one might realize. An MIT analysis of three months of credit card data records for 1.1 million people found that any individual can be identified with more than 90% accuracy by looking at just four purchases—even after

38. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity and risk associated with the data
39. Consumers have a right to reasonable limits on the personal data that companies collect and retain
40. Consumers have a right to secure and responsible handling of personal data.
41. Companies should be accountable to enforcement authorities and consumers for adhering to these principles; *See* Press Release, The White House Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
42. *Id.*
43. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.
44. *Id.*
45. *Id.*
46. Ian Allison, *Big Data, Big Problem: Could Wall Street See Insider Trading Lawsuits Over Selling Data Sets?*, NEWSWEEK (Oct. 11, 2017, 8:25 A.M.), https://www.newsweek.com/could-wall-street-see-first-legal-action-selling-data-sets-682188.

companies have "anonymized" the records.[47] "It is not surprising to those of us who spend our time doing privacy research," said outside expert Lorrie Faith Cranor, director of the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University.[48] "But I expect it would be surprising to most people, including companies who may be routinely releasing de-identified transaction data, thinking it is safe to do so."[49] The larger concern is that companies are building these permissions into the user agreements.[50] Unwittingly, consumers are signing on to be watched, analyzed, and stripped of their privacy. This cannot go on.

The GDPR accounted for this "anonymization myth," defining "personal data" more broadly than the U.S. definition for "personally identifiable information" (PII).[51] In the GDPR, the question is "whether a person can be identified on the basis of the data—essentially, can you reverse engineer the data or combine it with other data you have access to in order to identify an individual?"[52] PII, on the other hand, is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[53] While this *might* account for the anonymization myth, current regulation does not explicitly account for the possibility of aggregates being reverse engineered. Adopting the broader definition of the GDPR reduces the threat of "reverse engineering," preventing companies and data brokers from hiding behind anonymization.

This proposition is not perfect—nor does it purport to be. The most important thing right now is to have a jumping off point to create some semblance of accountability of data brokers and companies to consumers without stagnating in technological advancements in trading. The next

47. *See* Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh & Alex "Sandy" Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE, no. 6221, Jan. 30, 2015, at 536,http://science.sciencemag.org/content/sci/347/6221/536.full.pdf.
48. Seth Borenstein & Jack Gillum, *'Anonymized' Credit Card Data Not So Anonymous, Study Shows*, MIAMI HERALD (Jan. 29, 2015, 5:44 P.M.), https://www.miamiherald.com/news/nation-world/national/article8586050.html.
49. *Id.*
50. *See* Jeffrey D. Neuburger, et. al., *Big Data and Hedge Funds; An Emerging Trend with its Own Legal and Compliance Issue*, PROSKAUER ROSE (July 2017), https://www.wellsfargo.com/com/securities/markets/equity-sales/prime-services/publications/update-07-17/#data.
51. 2 C.F.R. § 200.79
52. Robin L. Barton, *How the GDPR Will Affect Private Funds' Use of Alternative Data*, 11 HEDGE FUND L.REP., June 14, 2018, no. 24, https://www.lowenstein.com/media/4468/sf1483-how-the-gdpr-will-affect-private-funds-use-of-alternative-data.pdf.
53. 2 C.F.R. § 200.79

section discusses how this proposition might impact demand side investment managers.

III. DEMAND SIDE: INVESTMENT MANAGERS

It would be naïve not to recognize the immense efficiency and profitability of utilizing alternative data in investment decisions.[54] That is why a group of asset managers spent $373 million in 2017 on datasets and new employees to parse through them, 60% more than the prior year.[55] It is also why alternative data spending is forecast to jump to $616 million in 2018, and $1 billion by 2020.[56] But as SEC Commissioner Kara M. Stein stated, "[o]ur financial system's growing dependence on vast amounts of data and the tools that analyze it are significantly changing our financial markets. Our financial regulations need to change as well."[57]

For the avoidance of doubt, use of alternative data does not fall within the ambit of insider trading—at least as the law currently stands. Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, on the basis of material, nonpublic information about the security.[58] As Dechert partner and former S.D.N.Y prosecutor Jonathan Streeter puts it, "if you can get comfortable" that any one of these elements has not been met, "you can go ahead and trade on it."[59] The private consumer information provided in these data sets is nonpublic and likely material, as evidenced by (a) funds' willingness to purchase the sets at such high subscription rates and (b) analysts' incorporation of the sets into their models.[60] The fiduciary duty element, however, is missing under the current regulatory landscape.

The question presented with respect to duty is, as Streeter states, "did someone do something they weren't supposed to do somewhere along the

54. *See* Stein, *supra* note 2.
55. John Manning, *Hedge Funds See Huge Potential in Alternative Data*, INTERNATIONAL BANKER (Oct. 22, 2018) https://internationalbanker.com/brokerage/hedge-funds-see-huge-potential-in-alternative-data/.
56. *Id.*
57. Stein, *supra* note 2.
58. 17 C.F.R. § 240.10b-5 (2017).
59. Jonathan Streeter, Partner, Dechert LLP, Address at the Battlefin Alternative Data Discovery Day Miami Panel 8 (10:09 – 10:29) (Jan. 19, 2018). Prior to coming to Dechert, Streeter was an Assistant United States Attorney for the Southern District of New York. He led the pivotal insider trading case against Raj Rajaratnam, co-founder of the Galleon Group.
60. *Id.* (10:43-11:30) ("if your portfolio managers and your analysts . . . put this information into their model, if you spent money buying it . . . you are proving that the information is material. The legal standard for materiality is 'would a reasonable investor consider the information important in their investment decision.")

chain from the origin of that data?"[61] In other words, when Consumer A went to Verizon to purchase a cell phone, did they agree that Verizon could sell their geolocation to Data Broker B who sells it to Hedge Fund C? If so, Verizon has rid themselves of a duty to keep that information confidential and hedge funds may trade at their leisure. With minimal legislative oversight, this is almost always the case. When companies slide data sign-off permissions into consumer terms and conditions, and a consumer has—unknowingly or knowingly—granted that permission, selling the data is perfectly legal. Under the proposed supply-side legislation, requiring opt-in permission from consumers would mean that consumers could choose whether their private information is sold or not. But, more important to the insider trading analysis, the proposed statutory language should classify any single holder of such information to be a fiduciary. Thus, should a company not implement opt-in provisions or sell the data in spite of express disapproval, a fund that purchases and trades on such information may now be subject to insider trading under the misappropriation theory.[62]

While funds are willing to take prophylactic measures to "play clean" now,[63] this likely will not last. In what fund managers have dubbed the "Wild West,"[64] investment managers will seek new ways to get ahead of the competition. Deloitte reported in 2017 that "[a]lternative data will likely transform active investment management (IM) over the next five years."[65] The company further contends that those who do not update their practices to incorporate alternative data will "be outmaneuvered by competitors that effectively incorporate alternative data into their securities valuation and trading signal processes."[66] It won't be long, then, before one fund turns the other cheek when the unlawfully obtained data is just too good to pass up.

In practice, it should not be difficult to ensure supply-side company compliance with the law—it can be as simple as a few additional questions in a due-diligence questionnaire (DDQ). In fact, many U.S. companies

---

61. *Id.* (14:00 – 14:50)
62. The misappropriation theory involves the breach by a corporate "outsider" entrusted with confidential information of his or her fiduciary duty to the source of that information. *See* United States v. O'Hagan, 521 U.S. 642, 652–53 (1997).
63. *See* Lindsay Fortado, Robin Wigglesworth & Kara Scannell, *Hedge Funds See a Gold Rush in Data Mining*, FINANCIAL TIMES (Aug. 28, 2017), https://www.ft.com/content/d86ad460-8802-11e7-bf50-e1c239b45787 ("Hedge funds such as Man Group and AQR capital posit, exclusive data sets may not be worth the legal risk or expense.").
64. *Id.*
65. DELOITTE CENTER FOR FINANCIAL SERVICES, *Alternative Data for Investment Decisions: Today's Innovation Could be Tomorrow's Requirement* (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-alternative-data-for-investment-decisions.pdf.
66. *Id.*

have already proven capable of complying with the GDPR. Peter Greene, partner and vice chair of the Investment Management group at Lowenstein Sandler, shed light on the minimal steps funds would need to take to comply.[67] The main requirement is that funds add a relevant addendum or compliant covenant to service agreements with any vendors that provide alternative data touched by the regulation.[68] If funds have lawfully obtained the data and have done due diligence to ensure the supplier is compliant with privacy laws (i.e., that they have obtained the proper representations from educated consumers), then there is no legal reason not to trade on that information. This practice will provide the necessary backstop to incentivize funds not to blindly purchase, exploit, and trade on unauthorized personal data.

CONCLUSION

When President Obama introduced the CPBR in 2012, he stressed that "it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times."[69] As alternative data continues to grow in value to companies, action is needed now more than ever. Future legislative efforts should supplement past ones in developing a series of requirements for companies that set a floor for privacy protections and impose a fiduciary duty on holders of such sensitive information. In order to rein in companies supplying the data and the hedge funds trading on it, legislators must take another swing.

67. *See* Robin L. Barton, *How the GDPR Will Affect Private Funds' Use of Alternative Data*, HEDGE FUND L. REP., June 14, 2018, no. 24, https://www.lowenstein.com/media/4468/sf1483-how-the-gdpr-will-affect-private-funds-use-of-alternative-data.pdf.
68. *See id.*
69. Press Release, The White House Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.