Unravelling the Gordian Knot for Data Trusts—The Next Leap Forward for Equity?

Kan Jie Marcus Ho*

The advent of the fourth industrial revolution has heralded new strategies for addressing the challenges of data governance. With data emerging as one of the penumbral hot button topics undergirding the evolution of digital technology, policymakers and regulators have been faced with an inevitable struggle—finding the best way to manage, utilize, and ensure the security of personal data, particularly when in the hands of corporate organizations. Hitherto, various top-down regulatory endeavors have emerged to address this challenge, such as the General Data Protection Regulation (GDPR) in the EU, and various sector specifics laws in the U.S. However, as recognized by several scholars, a top-down approach is insufficient to equip end-users with sufficient teeth to ensure protection of their personal data. This is because even with stringent data protection legislation, an asymmetry of power is often commonplace in the online service provider industry, which has led to misuse of personal data and exploitation of the end-user.

This being the case, there remains a critical need to uncover a plausible bottom-up approach for the purpose of re-jigging online service providers back into the realm of compliance. Therefore, this Article seeks to explore whether data trusts, and in particular, the principles undergirding Fiduciary Law and The Law of Trusts, could provide the way forward for establishing a workable structure to imbue end-users with individual rights of enforcement. After canvassing the modern confusion surrounding the substantive essence of a data trust, this Article seeks to take a three-part attack to support the proposition that fiduciary law may provide the way forward in holding online service providers to task vis-à-vis personal information of end-users, both in U.S and English law.

In Part II of this Article, I make the argument that an ad hoc fiduciary rationalization between online service providers and end-users suffices to imbue the end-user with a bottom-up workable enforcement mechanism that possesses some teeth in the U.S. This causes me to diverge from Balkin's seminal information fiduciary thesis, wherein he views information fiduciaries as a status-based fiduciary relationship. I do not agree that a status-based rationalization is appropriate, as this heralds rigid scope issues and further, applying a blanket rule is rather myopic. Having established the existence of an ad hoc fiduciary relationship vis-à-vis online service providers and its end-users, I then address any dissent against such a model, the most prominent of which being undergirded by Khan and Pozen's thesis. I point out that there are formative and substantive issues with the duo's attempt to defeat a fiduciary rationalization, thereby fully defending the existence of an ad hoc fiduciary rationalization in US Law.

Part III of this Article then seeks to transpose a fiduciary model into UK Law, in a bid to examine whether this sits well with modern English jurisprudence concerning fact-based fiduciary relationships. I contrast this against a traditional trusts model (analogous to what has been advanced by Delacroix and Lawrence) and conclude that a fiduciary model remains the better option in unravelling this Gordian knot. Finally, in Part IV of this Article, I seek to utilize various sector-specific case studies to "test" the viability of my proposed fiduciary model in light of the

* © 2023 Kan Jie Marcus Ho, LL.M. (Harvard) (Dean's Scholar Prize Winner); BA (Hons) (Law) (Hons) (Cantab) (First Class Honours). I am grateful to the anonymous reviewers for their comments on earlier drafts. Any errors remain my own.

current data protection framework in both the U.S. and the UK. In the final analysis, I conclude that a fiduciary rationalization is preferable for both jurisdictions to hold online service providers to account. As the fourth industrial revolution surges ahead, with data as its essential fuel lighting the way, establishing a workable bottom-up enforcement model would undergird end-users with more teeth and promote better data protection practices in the road ahead.

I. CHARTING THE PROBLEM 149
II. A FIDUCIARY RIPOSTE FOR U.S. LAW 154
  A. *The Concept of Information Fiduciaries* 155
    1. Balkin's Theory 155
    2. Testing the Limits 157
    3. Checking the Boxes of an Ad Hoc Fiduciary 159
    4. Justifying the "Information Fiduciaries" Theory Instead Through the Fact-Based Fiduciary Doctrine 160
  B. *Imposing Fiduciary Relationships Could Engender Unexpected Outcomes* 163
    1. The Fiduciary Model is Beset by Internal Tensions ... 164
    2. The Fiduciary Duty *viz.* Online Service Providers and End-Users Should Not Belong in the Realm of Fiduciary Law, for the Analogy with Professionals is Unconvincing 168
    3. Is This the End for Targeted Advertising? 171
  C. *The Scope of Fiduciary Duties of An Online Service Provider as an Ad Hoc Fiduciary* 173
    1. The Duty of Loyalty 173
    2. The Duty of Care 176
    3. The Subsidiary Obligations 177
  D. *Remedies and Conclusion* 179
III. A TRADITIONAL TRUSTS-BASED RIPOSTE FOR ENGLISH LAW? ... 180
  A. *The Counterattack Against a Fiduciary Model* 180
  B. *A Traditional Trusts Approach?* 184
    1. Advantages of the Present Proposal 185
    2. Justifying a Traditional Trusts Framework 187
      a. The Property Problem 187
      b. The "Relevance" Quandary 192
      c. Tentative Conclusion 195
  C. *An Ad Hoc Fiduciary Approach for English Law?* 195
  D. *Applying an Ad Hoc Fiduciary Framework for Online Service Providers in English Law* 198
  E. *Shaking the Substratum of the Fiduciary Doctrine* 203

IV. COMPLEMENTING EXISTING TOP-DOWN REGIMES TO ENFORCE EFFECTIVE DATA PROTECTION 207
A. English Law 207
B. U.S. Law 210
V. CONCLUSION 211

I. CHARTING THE PROBLEM

"The world is now awash in data[,] and we can see consumers in a lot clearer way[s]."[1] Max Levchin, co-Founder of PayPal, rightly points out that the data explosion of the fourth industrial revolution has heralded an infinite number of possibilities for businesses of tomorrow. But alas, every rose hides its thorns. Hidden within the undergrowth of the digital economy lies an inevitable Gordian knot, as increasing reliance on personal data collection by modern corporations renders a growing need to enforce strict data protection compliance standards.

It is undeniable that data collection undergirds the effective running of corporations in the present day. Take for example, Facebook, Google, and Twitter—juggernauts of the digital industry. These online service providers rely on collected data as a core fuel to generate insights and provide value to end-users.[2] Even for corporations outside of the digital sphere, data collection practices are increasingly picking up steam, as companies are starting to realize the value of unlocking insights within data. However, plentiful as the benefits of big data collection may be, the lacuna of unauthorized data use has eclipsed any excitement. Here, concerns remain as large companies continue abusing their position of power to the detriment of individual end-users. Certainly, as Lina Khan and David Pozen (Khan and Pozen) opine, actions contrary to a data subject's interests are commonplace and often materialize in the form of predatory advertising practices, including acts that not only "enabl[e] discrimination [and] induc[e] addiction," but further engender end-user's desire to share their personal data with third parties.[3] In this regard,

1. *Alchemy: The Strategic Data Transformation,* DELOITTE (2021), https://www2.deloitte.com/content/dam/Deloitte/it/Documents/strategy/2021DeloitteAlchemy.pdf [https://perma.cc/TY8Z-DVFK].

2. Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. 1183, 1226 (2016).

3. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 498 (2019). Khan and Pozen take a critical look at Balkin's proposal of online service providers as information fiduciaries, analyzing a range of purported substantiative problems and enforcement issues. *See id*.

regulators have performed a valiant endeavor to unravel this Gordian knot.

A mention of data protection in the United States or United Kingdom is likely to engender a discussion of the General Data Protection Regulation (GDPR), noted by Margret Taylor of the International Bar Association as the "gold standard for the protection of consumer information . . . usher[ing] in the world's toughest-ever privacy regime."[4] Although the United States has no analogous federal privacy law, the U.S. boasts a myriad of sector-specific data security laws with hundreds of general privacy and data security at a state-level.[5] For example, California has enacted more than twenty-five state privacy and data protection laws, including the recent California Consumer Privacy Act (CCPA).[6] The CCPA augments individuals with various privacy rights, which include the right to know the personal information collected, the right to delete personal information collected from them, the right to opt-out of the sale of their personal information, as well as the right to non-discrimination for exercising their rights imbued via the CCPA.[7]

At first glance, top-down regulatory mechanisms appear to act as effective bastions of personal data.[8] However, all that glitters might not be gold. What the regulatory mechanisms appear to promise in *form*, might not be what such mechanisms deliver in *substance*. Analyzing the GDPR as a key example, Sylvie Delacroix and Neil Lawrence (Delacroix and Lawrence) contend that there is a deficiency for individual "subjects to take the reins" in protecting their personal data.[9] This remains to be the case despite the GDPR imposing duties on corporations from the recognition that individual data subjects rarely find themselves in a

4. Margaret Taylor, *Data Protection: Threat to GDPR's Status as 'Gold Standard,'* INT'L BAR ASS'N (Aug. 25, 2020), https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED532 [https://perma.cc/9QHH-TVGR]. The GDPR features core tenets of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. *See generally* Council Regulation No. 2016/679, 2016 O.J. (L 119) 1 *and* Council Directive No. 95/46/EC, 1995 O.J. (L 281) 31.

5. *See, e.g.*, Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, §§ 6821-6827.

6. *See generally* Franz-Stefan Gady, *EU/U.S. Approaches to Data Privacy and the 'Brussels Effect,'* GEO. J. INT'L AFFS. 12 (2014).

7. *See* California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100—1798.199.100 (2018).

8. *See generally Data Trusts: A New Tool for Data Governance*, ELEMENTAI (2019), https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf [https://perma.cc/CP5H-UZSM].

9. Sylvie Delacroix & Neil D. Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIV. L. 236 (2019).

"position to bargain."[10] Thus, though the GDPR promises to serve as a cure to these poisons, empirically such legislation has not actually prompted substantive change within companies. Rather, corporations continue to navigate towards the boundaries of legal permissibility.[11]

Similarly, liberal democracies have hesitated to impose contractual restrictions to promote compliance with data governance as such a restriction is at odds with the "*raison[] d'être* sof liberal democracies."[12] Why is this so? As a threshold matter, it is important to note that situations of power asymmetry frequently arise between an end-user and a large online service provider.[13] End-users are often forced into contractual regimes of data protection that are drafted by large online companies. Typically, such contractual regimes are crafted in ambiguous and opaque ways, thereby tipping the scales to favor the large online companies. Thus, data subjects are forced to live under an illusion of free choice, subject to contractual regimes that more often than not favor the companies.[14]

Further, Delacroix and Lawrence note that an imbalance of power in the modern online industry has been exponentially growing for the past decade, that is underscored by a lack of professional code of conduct that could potentially curb the behavior of online service providers.[15] Presently, data protection laws have not forced online service providers to *inherently* change their business models, establishing a continuing trend of data abuse with no end in the foreseeable future.[16] These mechanisms, thus, fail to solve the power asymmetry problem between data controller/businesses and data subjects/consumers, placing end-users between a rock and a hard place.

However, a potential escape rope might present itself in the use of data-trusts as a mechanism to solve the current power imbalance. If successful, this might prompt a re-jig towards a more "bottom-up" approach of enforcement from the position of the end-user. Coined in 2004 by Lilian Edwards, a *data trust* was conceptualized as a model of governance, granting "data subject[s] . . . an individual right of action against an abusive data collector."[17] However, loose terminology has led

10. *Id.* at 239.
11. *See id.*
12. *Id.*
13. Christine Rinik, *Data Trusts: More Data than Trust? The Perspective of the Data Subject in the Face of a Growing Problem*, 34 INT'L REV. L. COMPUTS. & TECH. 342, 351 (2020).
14. *Id.* at 352.
15. *See* Delacroix & Lawrence, *supra* note 9, at 240.
16. *See id.*; *see also* Rinik, *supra* note 13, at 352.
17. Lilian Edwards, *The Problem with Privacy*, 18 INT'L REV. L. COMPUTS. & TECH. 309, 329 (2004).

to much confusion, with various models emerging in the past decade that range from the traditional idea of the *settlor-beneficiary* trust to a regulatory model with additional contractual obligations.[18]

To understand the current developments in this area, three sources may be of interest. The first source comes from a report developed by the United Kingdom, *Growing the Artificial Intelligence in the UK*, which suggested data trusts as a way forward in facilitating the "sharing of data between organisations holding data and organisations looking to use data" for various purposes.[19] Interestingly, this report viewed such trusts not as a "legal entity or institution," but rather as "a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe, and equitable way."[20] To create a tenable framework, the report suggests the development of an administrative body, the Data Trusts Support Organisation (DTSO), to serve as a *default trustee*, thereby providing both regulatory oversight and expansion of such trusts. *Prima facie*, the premise of data trusts appears promising, particularly considering the UK's report.

The second source, however, provides a more cautionary narrative in the use of data trust. Sidewalk Labs (SL) provided a report of its proposal to develop Quayside, a "smart city" neighborhood in Toronto.[21] Here, undergirding the SL's model was a proclaimed civic data trust, in which SL claimed to be a "model for stewardship and management of data and digital infrastructure [which would] approve[] and control[] the collection and use of data for the benefit of society and individuals."[22] At the core of this model, urban data was to be disclosed, while allowing public access to the data itself.[23] This open data structure, however, quickly exposed an underlying faux pas encompassed within the model. If the data pool contained information lacking any personally identifiable data, this data *could be* automatically anonymized, rendering it impossible

18. *Data Trusts*, *supra* note 8, at 10, 14.

19. Dame Wendy Hall & Jérôme Pesenti, *Growing the Artificial Intelligence Industry in the UK*, GOV.UK (Oct. 15, 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf [https://perma.cc/9KT2-XZMW].

20. *Id.* at 46.

21. *Digital Governance Proposals for DSAP Consultation*, SIDEWALK LABS (Oct. 2018), http://quaysideto.ca/wp-content/uploads/2019/04/DSAP-Digital-Governance-Proposals-Presentation-October-18-2018.pdf [https://perma.cc/C779-2KVY].

22. *Id.* at 12.

23. *Id.* at 13.

to trace individuals whom data was collected.[24] Critics noted that the model was peppered with incoherency, "pursu[ing] two different data governance strategies simultaneously."[25] Though the model promoted "a heightened level of protection for data, it did not incorporate additional protective norms like fiduciary obligations."[26] This model, thus, was beset by internal tensions of "accountability and oversight" versus that of data protection.[27] Ultimately, the civic data trust was not feasible in providing a secure bottom-up enforcement mechanism, thereby dragging it into the depths of unworkability.

The third source, a report by the Open Data Institute (ODI), revived the continuing debate of data trusts. There, ODI sought to "solve one of the fundamental problems faced when utilizing machine learning," this being the problem of data sharing.[28] Interestingly, ODI adopted a two-fold stance in denying trust law as an "appropriate legal structure" for data trusts, citing two reasons to substantiate their argument.[29] First, ODI argued that a "legal trust *must be run* for the benefit of the beneficiaries, *not* the wider public."[30] Though noting a "charitable trust" as a sole exception, ODI asserted that "[f]or an ordinary legal trust, trustees are required only to consider the collective interests of the beneficiaries when dealing with trust property."[31] Second, the ODI argued that "trustees are obliged not to use the property of the legal trust in a way which generates benefits for themselves," subject to any contrary provision in the trust deed.[32] This, however, is fatal to the trust approach as both "providers and users of data" are inevitably encumbered by the prospect of "envisaging benefits for themselves [through the act] of data sharing."[33] Thus,

24. Moreover, concerns were levied about the use and control of the public's personal data as SLP was a subsidiary of Alphabet Inc. *See* Joshua Brunstein, *Alphabet's Sidewalk Labs Offshoot Is Now a Unicorn*, BLOOMBERG (Feb. 2, 2022, 6:00 AM), https://www.bloomberg.com/news/articles/2022-02-02/alphabet-googl-sidewalk-labs-offshoot-sip-is-now-a-unicorn [https://perma.cc/95W5-YUXK].

25. Lisa M. Austin & David Lie, *Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Lab's Urban Data Trust*, 19 SURVEILLANCE & SOC'Y 255, 258 (2021).

26. *Id.*

27. *Id.* at 259.

28. Christopher Reed, *What is a Data Trust in Legal Terms?*, *in* DATA TRUSTS: LEGAL AND GOVERNANCE CONSIDERATIONS 10 (Apr. 2019), https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf [https://perma.cc/N3GN-EEKQ].

29. *Id.* at 8.

30. *Id.* at 12 (emphasis added).

31. *Id.*

32. *Id.* (footnote omitted).

33. *Id.*

companies, especially those providing online services, are disincentivized from jumping onto the data trusts bandwagon from the get-go.[34] Ultimately, requirements reducing the benefits normally enjoyed by trustees in such a role, here the trustees being the online service providers, likely represents the Achilles' heel to any model of data trusts taking flight in the foreseeable future.

The problems presented thus far, when taken together, inspire the research question of this Article. In this Article, I seek to chart an inquiry into whether data trusts, utilizing foundational principles in the law of fiduciary and trusts, might prove worthy in crafting the golden key to unravel the Gordian knot that currently plagues data protection. First, I will analyze two dominant models of data trusts—the aforementioned traditional trust model and Jack Balkin's information fiduciaries model. Here, the Article highlights and distinguishes the weaknesses in both models, and instead, advocates for a novel *ad hoc* fiduciary model as the way forward. As will be shown in Part II and III of this Article, an *ad hoc* fiduciary model serves to undergird the end-user with a workable *bottom-up* approach and ushers in a fundamental re-jig of the current unsatisfactory law in the United States and United Kingdom governing the practices of online service providers. Ultimately, this Article concludes that the proposed *ad hoc* fiduciary solution sufficiently seizes the bull by its horns, giving end-users a (proverbial) bottom-up lasso to stop online service providers from running amok with end-users' personal data amidst the rodeo of the fourth industrial revolution.

II. A FIDUCIARY RIPOSTE FOR U.S. LAW

In the United States, Daniel Kelly describes that courts have recognized a variety of *status-based* fiduciary relationships.[35] Outside of these "established relationships," case law has recognized an *ad hoc* fiduciary relationship in certain *fact-based* scenarios that the law deems sufficient to engender a fiduciary relationship. This recognition of such *ad hoc* relationships, however, has heralded uncertainty, as underscored by the court's "bewilderingly disparate characterizations" of such relationships when analyzing whether a fiduciary relationship exists.[36]

34. *Id.*

35. Daniel B. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW (Evan J. Criddle et al. eds., 2019) (describing the recognized fiduciary relationships such as the principal-agent, the trustee-beneficiary, and the corporate director-shareholders relationships).

36. Paul B. Miller, *The Identification of Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW *supra* note 35, at 374.

Given the "disparate characterizations" engendered by the courts, is there be any possible way of charting a way through the woods? In the context of online service providers, the ability to identify with consistency *when* an *ad hoc* fiduciary relationship exists may be especially valuable. Here, if *ad hoc* fiduciary relationship was established, online services providers would necessarily be tasked with fiduciary duties to end-users in the protection of personal data.

A. The Concept of Information Fiduciaries

1. Balkin's Theory

Prior to the advent of the fourth industrial revolution, the term "information fiduciaries" was pioneered by Kenneth Laudon to describe the relationship between online platforms and customers depositing data into such platforms.[37] Characterizing the traditional nature of such a relationship, Laudon suggests that information fiduciaries "accept deposits of information from and seek to maximize the return on sales of that information in national markets or elsewhere in return for a fee, [some] percentage of the total returns."[38] In 2014, Laudon's embryonic theory was further nurtured by Jack Balkin when Balkin utilized the information fiduciary doctrine as a way to "protect digital privacy while not running afoul of the First Amendment."[39] Subsequently, Balkin matured his information fiduciary theory, advocating for a fiduciary relationship to be recognized between online service providers and end-users due to *social relationship* engendered between online service providers and end-users.[40] Additionally, Balkin notes that traditional support of top-down regulatory enforcement models have missed this special relationship, consequently leading scholars to dismiss fiduciary law as a tenable mechanism for bottom-up enforcement.[41] Thus, Balkin therefore asserts that it is timely for a radical overhaul of the current data protection debate.[42] Balkin supports his assertion by analogizing online service providers to other professional service industries, in which such professionals face tort liability arising "in the context of [their] contractual

37. *See generally* Kenneth C. Laudon, *Markets and Privacy*, 39 COMMS. ACM 92 (1996).

38. *Id.* at 101.

39. Jack M. Balkin, *Information Fiduciaries in the Digital Age,* BALKINIZATION BLOG (Mar. 5, 2014, 4:50 PM*),* http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/2D2S-ENDR].

40. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1205.

41. *Id.*

42. *Id.*; *see also* Jack M. Balkin, *Free Speech Is a Triangle*, 118(7) COLUM. L. REV. SYMP. 2011, 2049 (2018).

relationships."[43] Here, Balkin posits that tort law is not the only solution to hold professionals accountable for the misuse of personal data and suggest that an easier, more elegant solution exists.[44] Forming the substratum of his thesis, Balkin posits the solution may be found in fiduciary law.[45]

In other professional service industries, such professionals hold a "special relationship[] of trust and confidence with their clients."[46] Thus, Balkin asserts a fiduciary relationship ought to arise. Acting as an alternative mechanism to impose liability for data misuse by professionals, Balkin suggests such a model may in fact usher in a higher and more secure standard across industry.[47] Following this argument to its logical conclusion, and supposing that a fiduciary duty is made out between the professional and an end-user, online service providers will be held accountable under the obligations posed by the duty of care and loyalty.[48] In sum, Balkin views fiduciary law as simply more elegant and extensive in mandating the protection of personal data.

Balkin's analogy draws strong hints to Daniel Kelly's analysis on *fact-based fiduciaries*, given the level of intimate trust and confidence between the two entities.[49] However, Balkin takes a different path, arguing that an "information fiduciary" must possess a "[subsisting] relationship with another," and thereafter "has taken on special duties with respect to the information they obtain in the course of the relationship."[50] Thus, such a relationship is a uniquely *status-based* category. Though Balkin discusses, for example, how "Facebook has three different kinds of duties toward its end users," he does not fully elaborate how such companies could be held liable.[51] When end-users pass their personal data to an online service provider, there is no existing *status-based* fiduciary category recognizing a purchaser and vendor

43. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1205-06. Balkin further notes that in other professional service industries, courts have found "professional malpractice and professional breach of duty" even in the absence of a contractual agreement when such professionals have misused personal data, *see id*. at 1206.

44. *See id*. at 1205.

45. *See id*.

46. *Id.*

47. *Id.*; *see also* Balkin, *Free Speech Is a Triangle*, *supra* note 42, at 2049.

48. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1221.

49. *See* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 9.

50. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1209 (footnote omitted).

51. *See* Balkin, *Free Speech Is a Triangle*, *supra* note 42, at 2051-53.

relationship. Here Balkin's thesis falls out of rhythm. Balkin fails to both justify *where* this subsisting relationship could come from between the interaction of online service providers and end-users as well as *what* kind of information should be protected.[52] Further, Balkin fails to cite the trigger as to *when* such providers become liable or *how* this subsisting fiduciary relationship is generated.

Critiquing his own theory, Balkin acknowledges an issue of the scope of duties imposed to information fiduciaries, "especially if we want [those] duties to be consistent with the First Amendment."[53] Therefore, Balkin suggests that *information fiduciaries* are inherently different from other *status-based* traditional categories.[54] Here, Balkin provides three distinguishing facets on information fiduciaries: (1) expectations of trust by consumers;[55] (2) nature of the business enterprises themselves;[56] and (3) proactive obligations in harm prevention.[57] Simply put, the scope of duties that information fiduciaries are held responsible to are different compared with the traditional categories. Ultimately, is Balkin's conclusion justified? I argue not. Even if his status-based rationalization were to apply to online service providers as he claims, the rigid scope issues that he necessarily concedes renders such a model nothing but otiose. Something different is needed.

2. Testing the Limits

For online service providers, it cannot be denied that information forms the oil to power said organizations, especially when data generation and analytics increasingly forms the core business and compensation model in the digital era. It has been well established that upon winding up or liquidation of an online service provider, the data and insights

52. *See generally* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2.

53. *Id.* at 1225.

54. *Id.* at 1225-26.

55. *Id.* at 1227 ("Because personal data is a key source of wealth in the digital economy, information fiduciaries should be able to monetize some uses of personal data, and our reasonable expectations of trust must factor that expectation into account.").

56. *Id.* at 1228 ("We might not want to impose comprehensive obligations of care on digital companies like Google, Facebook, or Uber. Their business are quite different from those of doctors, and they do not hold themselves out as taking care of end-users in general.").

57. *Id.* at 1229 ("Although at some point [an online service provider's] interest in promoting disclosure and production of content may create a conflict of interest between companies and end-users, we should not assume that online service providers have a positive obligation to stop asking people to reveal more of themselves in social media.").

generated are often what is most valuable.[58] Here, an online service provider is often faced with this question—should it choose to *protect* end-user data, or *exploit* it to acquire further value?[59] This is the classic *conflict of interest* situation that Equity Law is so familiar with, and it remains critical to develop a working framework.

What might one way out of the woods be? Presently, no *status-based* fiduciary relationship vis-à-vis online service providers and end users is recognized by the law, other than Balkin's existing theory. As suggested earlier, it might be possible to augment this situation with a fiduciary relationship on an *ad hoc* basis, similar to Judge Richard Posner's approach in *Burdett v. Miller*.[60] Robert Sitkoff correctly highlights that "categorical fiduciary relationships do not exhaust the universe of potential agency problems," and recognizes "[a]n agency problem [could] arise in other relationships, depending on the circumstances."[61] In the context of online service providers then, an agency problem arises in the aforementioned conflict of interest situation, whereby online service providers are necessarily imbued to exploit data for business value. Perhaps, this might be the way forward.

Here, the alarm bells seem to be ringing at full blast. Balkin ushers in the same concern, viewing it as fatal to simply pass the reins of control to the invisible hands of market forces to re-jig the right result.[62] According to him, this is because market forces are ultimately plagued by the problem of asymmetric information. On the one hand, online service providers are tempted to hide their "operations, algorithms, and [data] collection practices" from other stakeholders, in a bid "to prevent free-riding" practices or unintended parties from accessing proprietary data practices.[63] On the other hand, end-users are completely lost and unaware of their rights, there being no certain way of predicting the differing data practices vis-à-vis different online services providers.

Top-down regulatory regimes like the GDPR or sectorial protection in the United States rarely cut any ice against this situation, as Balkin notes that such companies are often disposed to present end-users of the upper limits of what is legal, such that "end-users are largely dependent

58. *See id*.

59. *See id*.

60. *See* 957 F.2d 1375, 1381 (7th Cir. 1992).

61. Robert Sitkoff, *An Economic Theory of Fiduciary Law*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 200 (Andrew S. Gold & Paul B. Miller eds., 2014); *see* Deborah A. DeMott, *Fiduciary Principles in Trust Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 29.

62. *See* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1226.

63. *Id.*

on the good will of these companies not to abuse their personal information."[64] Here, there is still an inherent imbalance of power when an end-user agrees to the license of an online service provider or signs a contract determining his data rights. Therefore, due to (i) "significant asymmetries of knowledge and information," (ii) challenges by end-users in verifying actual data practices, (iii) a gap in understanding *how* information is *actually* used, and (iv) monitoring challenges, Balkin believes that a top-down approach fails.[65]

Largely, I agree that Balkin is on the right track, though he skips over certain nuances such as how a fiduciary relationship can be created. Rather, Balkin simply states that anyone "who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship" is an information fiduciary.[66] This, however, does not justify how fiduciary relationships arise between the online service providers and end-users. An online service provider is not necessarily a professional all the same, contrary to his view. Hence, a *status-based* imposition, just like a rubber stamp, might prove unwieldy to rationalize the law.

This being the case, I will therefore once again tackle the existence issue, diverging from Balkin insofar as analyzing how the fiduciary relationship between an online service provider and an end-user is created. Simply put, my starting point is through an *ad hoc* fiduciary rationalization. U.S. law in the *ad hoc* fiduciary domain has sufficiently developed to the point where the general principles can, and probably will embrace our tricky context. I therefore begin by discussing the black-letter triggers for *fact-based* fiduciary relationships in U.S. law.

3. Checking the Boxes of an Ad Hoc Fiduciary

Kelly suggests that an ad hoc fiduciary classification might instead chart a better path through the fog of confusion.[67] According to Kelly, the common thread linking the trio might be through a *principal-agent* analysis. From the perspective of a *principal*, Kelly highlights that a "court is more likely to conclude . . . a relationship is 'fiduciary' if a

64. *Id.* at 1227.

65. *Id.*

66. *Id.* at 1209 (footnote omitted).

67. *See* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 6-11 (describing the relevant factual considerations in each case); *see e.g.*, Burdett v. Miller, 957 F.2d 1375, 1381 (7th Cir. 1992); Wiener v. Lazard Freres, 241 A.d.2d 114, 121 (N.Y. App. Div. 1998); Patsos v. First Albany Corp.,741 N.E.2d 841, 848 (Mass. 2001).

principal places *confidence and trust* in the agent; if a principal lacks *expertise, knowledge, sophistication, or experience*; or if a principal *depends or relies heavily upon the agent's advice or judgment*."[68] On the *agent* side of the fence, Kelly notes that a "court is more likely to conclude a relationship is 'fiduciary' if an agent has *significant discretion* over the principal or the principal's property; if an agent has *particular expertise, knowledge, or trustworthiness*; if an agent exhibits *influence, superiority, or dominance* over the principal."[69] Yet, Kelly notes that other scholars have emphasized inconsistent findings in such relationships, as the goalposts containing the triggers continue to shift with each subsequent case.[70] Likewise, Kelly notes other scholars acknowledge the gaping lacuna created by this "deep inconsistency," but nevertheless "suggests the common elements [which arise in *fact-based* fiduciary situations] are trust or confidence, . . . [alongside] the resulting domination" of one party over another.[71]

I accept that the *ad hoc* doctrine may not seem sufficiently certain, unlike Balkin's definite stamp of approval on terming anyone who holds information *and* is a fiduciary to be an information fiduciary. The benefit of rationalizing from the *ad hoc* doctrine is that it allows us to begin from first principles. Though potentially seen as ambiguous, it is my view that there remain sufficient earmarks to justify a fiduciary relationship pertaining to the management of an end-user's personal data, particularly in light of the common traits.

4. Justifying the "Information Fiduciaries" Theory Instead Through the Fact-Based Fiduciary Doctrine

As opposed to Balkin's *status-based* categorization of information fiduciaries, I therefore herald a different fiduciary approach to solve the existence problem. Here, I argue that the context of online service providers particularly benefits from previously discussed triggers for an *ad hoc* fiduciary relationship. Because of the increasing amount of trust end-users place in online service providers, and the evolving expertise of online service providers regarding privacy law and practices, an *ad hoc*

68. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 9 (emphasis added); *see id*. (describing the similar reliance of an unsophisticated party relying on the expertise of a professional present in *Burdett* and *Patsos*).

69. *Id*. (emphasis added).

70. *Id*. at 10 (footnote omitted).

71. *Id.* (quoting D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399, 1413-14 (2002)) (internal citations omitted)).

fiduciary is beginning to arise as a far more likely phenomenon in most modern contexts involving online service providers.

The starting point is that the ubiquitous nature of digital companies and the increasing requirements to collect personal data has "provide[d] multiple opportunities for . . . continuous surveillance . . . that monitors and collects data."[72] Such organizations, augmented with an end-user's personal data, are often able to leverage on big-data analytics and strategic advertising to exploit end-users.[73] Subject to any top-down regulations or contractual obligations, end-users are often left stranded as the vulnerable party.[74] Indeed, we do not go a day without obtaining our modern services and experiences from digital companies, and the transfer of personal data has become a customary norm.[75]

What is problematic here is that such data is often channeled into a supposed "black box" of algorithms, containing a complex interface system that prevents end-users from understanding how exactly their personal data is being used.[76] Indeed, a study by Aleksandra Kuczerawy and Fanny Coudert highlighted that "privacy settings can play a great role in privacy protection" yet "[t]he whole problem is the way the tool is used."[77] Likewise, Katharine Sarikakis and Lisa Winter's study supports this position, recognizing that "recent case studies of the usage of SNSs [Social Networking Websites] suggest that users overestimate their knowledge and understanding of privacy laws and policies and that this deficit extends to matters linked to technologies, as well as to policies about privacy, trafficking of personal data, and fundamental rights."[78]

72. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1379 (2017).

73. *See id*. at 1381.

74. *See* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1222. This phenomenon become even more prevalent within the context of the Covid-19 pandemic, which caused a radical shift towards an online-focused paradigm. *See* Yan Xiao & Ziyang Fang, *10 Technology Trends to Watch in the COVID-19 Pandemic*, WORLD ECON. F. (Apr. 27, 2010), https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth [https://perma.cc/8QS9-ED75].

75. *See* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1185.

76. *See* Aleksandra Kuczerawy & Fanny Coudert, *Privacy Settings in Social Networking Sites: Is It Fair?*, *in* PRIVACY AND IDENTITY MANAGEMENT FOR LIFE 231, 235 (Simone Fischer-Hubber et al. eds., 2011).

77. *Id*. at 240.

78. *See* Katharine Sarikakis & Lisa Winter, *Social Media Users' Legal Consciousness about Privacy*, 3 SOC. MEDIA & SOC'Y 1, 3 (2017) (citations omitted). Sarikakis and Winters further note that end-users coped with such knowledge deficiencies by restricting their usage of such services, suggesting a "decisional dimension of privacy . . . in a situation where feelings of immobilization and deprivation of choice prevail," *id*. at 11 (citing STEFANO SCOGLIO, TRANSFORMING PRIVACY: A TRANSPERSONAL PHILOSOPHY OF RIGHTS (1998)).

Further, there seems to be an issue related to end-users overall desire to negotiate, stemming in part from a both a lack of a "either formal privacy law . . . or private T&C policies" on the platforms of online service providers.[79] Put simply, it seems that end-users are simply surrendering their rights to online service providers, accepting that this is how things operate in the digital world. End-users of today are fighting a losing battle against online service providers—lacking an alert system as to how data practices are constantly being changed by their online service providers, such users are left stranded on the creek with minimal options.[80]

Taken together, the vast power divergence between online service providers and end-users is obvious. It is therefore apt to now examine Kelly's factors for determining an *ad hoc* fiduciary relationship.[81] Analogizing Kelly's findings to end-users and service providers, on the *agent's end*, end-users, here being the principals, are placated to place (i) "*confidence and trust*" in online service providers, (ii) "*lack[] expertise*" in privacy laws, and (iii) typically "*rel[y] heavily*" on privacy policies stated on an online service provider's website.[82] On the *principal's end*, online service providers, acting as the agents, are (i) given "*significant discretion*" over the end-users' personal information, i.e., property, (ii) possess "*particular expertise*" in negotiating favorable policies to use end-users' data, and (iii) "*exhibit superiority*" over end-users in their ability to lobby for favorable regulations of data.[83] Moreover, online service providers do not necessarily comply with top-down regulatory frameworks. For example, studies have looked at the privacy notices on websites.[84] Here, an "international sweep [of privacy notices] found that 23% of the sites had no privacy policy at all, and of those that did, a third were considered as difficult to read, and many were not tailored to the website."[85] Thus, some online service providers may be living on the edge and consistently exercising superiority over their end-users by exploiting their lack of clarity vis-à-vis their data protection rights.[86] Here, an imbalance on the facts is clear .

79. *Id.* at 11.

80. *See id*. at 11-12.

81. *See* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 9.

82. *Id*. (emphasis added).

83. *Id*. (emphasis added).

84. *The Commercial Use of Consumer Data*, CMA ¶ 4.145, at 138 (June 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf [https://perma.cc/N7XR-9FU7].

85. *Id*.

86. *See* Sarikakis & Winter, *supra* note 78, at 3.

Thus far, this Article has shown that imposing a *fact-based* fiduciary relationship between online service providers and end-users in the context of managing personal data is justified and consistent with legal doctrine. Balkin's information fiduciary theory, though convincing, is straddled by a rigid status-based rationalization, restricting Balkin to construe the scope of duties of an information fiduciary in an artificial way. Likewise, Balkin's information fiduciary theory does not align well with situations where there is no existing and recognized fiduciary relationship. Therefore, the proposed *ad hoc* fiduciary rationalization does well to unravel the Gordian knot in a far more elegant way. As this Article has diverged from Balkin in this respect, the scope of the duties will necessarily be different as well. The next subsection tackles what duties ought to undergird an *ad hoc* online service provider fiduciary, in a bid to produce a workable model.

B. Imposing Fiduciary Relationships Could Engender Unexpected Outcomes

Currently, a *fiduciary model* for online service providers with end-users appear to be justified. Though I disagree with Balkin's thesis, our common starting point of a fiduciary duty renders it sensible to examine any existing dissent against his claims, which may likely be found in Khan and Pozen's reply to Balkin's proposal.[87]

Khan and Pozen shake the substratum of Balkin's *information fiduciary* model, flanking their riposte with three key arguments.[88] First, the duo asserts that the *fiduciary model* is beset by internal tensions because there is no way to reconcile the fiduciary duty that management owes to end-users for collecting their personal information *and* the fiduciary duty that management owes to its shareholders.[89] Second, the duo takes issue with Balkin's analogy to professionals, such as lawyers and doctors, asserting that this is not the case for online service providers.[90] Third, they argue that Balkin's analogy "risks obscuring the

87. *See generally* Khan & Pozen, *supra* note 3.

88. *See id*. at 508-10.

89. *See id*. at 508 ("The fundamental flaw in this argument, however, is that it runs counter to the prevailing understanding of Delaware doctrine . . . .").

90. *See id*. at 510 ("The one thing that does not vary . . . is that the fiduciary always must act in the customer's best interest . . . . Abandon this core tenet, and it is unclear what is left of the legal analogy to doctors, lawyers, accountants, and estate managers.").

contingent and constructed character of the power imbalances that exist between ordinary individuals and the major online providers."[91]

Here, Khan and Pozen's second counterattack proves interesting—and likely supports the proposed thesis in this Article. Nevertheless, I must first address arguments one and three, as these arguments directly target the weakness of a fiduciary-related model. In making this assertion, I present three rejoinders to prompt a re-jig back to a fiduciary approach.

1. The Fiduciary Model is Beset by Internal Tensions

Khan and Pozen initially assert that Balkin's model, or any *fiduciary sort of rationalization* for that matter, "requires consideration of . . . legal status quo faced by the relevant companies."[92] The duo points out that most online service providers are incorporated in Delaware.[93] Section 141(a) of Delaware's General Corporation Law (DGCL) imbues onto the board of directors the power to manage "[t]he business and affairs" of a corporation.[94] Yet, directors are still charged with acting in "the best interests of the corporation's stockholders."[95] This, in turn, heralds an inevitable clash between the fiduciary duty engendered as a result of being a steward of personal information and the fiduciary duty to stockholders to maximize profits. Additionally, Khan and Pozen argue that self-regulation by corporations, though resonating the best interests of stockholders, is not an effective means to regulation such corporations.[96] Here, the duo cites evidence suggesting that online service providers scarcely subscribe to this approach.[97] Rather, shareholder primacy ought to remain victorious at the end of the day because this is what companies like Facebook currently believe.

Against the duo, I contend that this is nothing but a bark up the wrong tree. Taking their first counterattack by the horns, I argue that the

91. *Id.* at 519; *see id.* ("[I]mbalances that stem both from the business model these firms employ and from the market dominance they enjoy . . . foreclosing a broader discussion about interventions that might prevent those imbalances from arising in the first place.").

92. *Id.* at 503.

93. *See id.* (listing service providers incorporated in Delaware).

94. *See generally* DEL. CODE ANN. tit. 8, § 141(a)(2020).

95. Leo E. Strine, *The Dangers of Denial: The Need for a Clear-Eyed Understanding of the Power and Accountability Structure Established by the Delaware General Corporation Law*, 50 WAKE FOREST L. REV. 1, 13-14 (2015).

96. *See* Khan & Pozen, *supra* note 3, at 508.

97. *See id.* ("The fact that corporations like Facebook have persistently declined to self-regulate along such lines, however, suggests that their boards do not see these reforms as likely to enhance firm value or shareholder wealth either in the short term or in the long term." (footnote omitted)).

duo has made an incorrect assumption that the duty of privacy is inherently conflicted with the duty to maximize shareholder value. Akin to the idea that Facebook *does not* represent all online service providers, it does not stand that Facebook's management continues down a similar route of denial. A single company's practice is not representative of the industry at large or other industries completely.[98] Khan and Pozen appear to labor under the assumption that most businesses are primed to churn out pollutants into digital "streams," while positing that existing regulation is inadequate to prevent "negative externalities" to the public generally.[99]

Moreover, Khan and Pozen note that critics argue that information fiduciaries "would require modification of companies' existing fiduciary duties to accommodate new duties to users."[100] However, the duo fail to illustrate how "a board [of directors'] . . . good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's central compliance risks"[101] would necessarily reduce shareholder value.[102] As Balkin quips, the problem would be solved if there was a Delaware statute *relevant* to privacy which would *preempt* the fiduciary duties to end-users over that of stockholders.[103] Still, this is not to say that compliance with a fiduciary duty to ensure adequate data protection would not maximize shareholder value. For example, consider emerging trends vis-à-vis corporate governance in the wake of the environmental,

98. For example, we may consider business practices and the effect of other areas of law. In 2020, a study examined whether corporation profit from breaking the law in the context of environmental pollutants. Nathan Atkinson, *Do Corporations Profit from Breaking the Law* 23 (ETH Zurich Center for Law & Economics, Working Paper, 2020). There, Nathan Atkinson found "that if corporations can profit from breaking the law, they will do so," *id*. at 23. This blasé attitude perhaps stems from the fact that "whole penalties for small violations are generally greater than the economic benefit of noncompliance, the benefits of noncompliance far outweigh penalties imposed for large violations," *id*. Likewise, another study reported that while 50% of rivers were polluted by large industrial corporations in the United States, only 12% of these corporations reported setting "pollution reduction targets." CDP, CLEANING UP THEIR ACT: ARE COMPANIES RESPONDING TO THE RISKS AND OPPORTUNITIES POSED BY WATER POLLUTION? 9 (2019), https://cdn.cdp.net/cdp-production/cms/reports/documents/000/005/165/original/CDP_Global_Water_Report_2019.pdf?1591106445 [https://perma.cc/XXD4-JG45].

99. *See* Khan & Pozen, *supra* note 3, at 539 ("A pollution perspective helps to highlight why private law solutions are inadequate to the nature of the threat." (footnote omitted)).

100. *Id*. at 509; *see id*. ("Facebook, Google, and Twitter would, as a rule, have to temper their duties to users with a higher duty of loyalty to shareholders.").

101. Marchand v. Barnhill, 212 A.3d 805, 824 (Del. 2019).

102. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134(11) HARV. L. REV. F. 11, 23 (2020).

103. *Id*. (emphasis added).

social, and governance (ESG) movement.[104] Here, Dorothy Lund and Elizabeth Pollman posit that "investors started to accept the notion that integrating ESG measures could mitigate risk and create shareholder value."[105] Simply put, the interests of shareholders are changing. In 2021, Chris Marsh and Simon Robinson highlighted in their study that "[t]he kinds of things [businesses] are focused on—namely . . . data protection and privacy—are becoming more important factors in social and governance measures."[106] Interestingly, Marsh and Robinson noted that for consumer data privacy, "[n]early half (46%) of consumers ha[d] reservations about sharing their personal data online, yet only 8% of businesses report[ed] having a dedicated data privacy team" that addressed privacy issues.[107] Moreover, Marsh and Robinson reported that "71% of merchants cited a rise in their customers' expectations of their organization."[108]

Ultimately, Khan and Pozen's first counterattack simply places the cart before the horse and ignores changes taking place in the world of corporations.[109] As noted, shareholders are increasingly recognizing ESG practices.[110] Further, it is not true that abiding by fiduciary obligations to end-users' privacy practices inherently chafes against a fiduciary duty owed to shareholders. Ultimately, this trend suggests a fundamental re-jig may be taking place in corporate law.

---

104. *See also* Dorothy S. Lund & Elizabeth Pollman*, The Corporate Governance Machine*, 121 COLUM. L. REV. 2563, 2612-15 (2021).

105. *Id.* at 2614; *see generally Who Cares Wins Conference*, *Investing for Long-term Value: Integrating Environmental, Social and Governance Value Drivers in* ASSET MANAGEMENT AND FINANCIAL RESEARCH, (Aug. 25, 2005).

106. Chris Marsh & Simon Robinson, *ESG and Technology: Impacts and Implications*, S&P GLOBAL MARKET INTELLIGENCE III (2021), https://www.spgloBal.com/marketintelligence/en/documents/451-esg-and-tech-dckb-report.pdf [https://perma.cc/A36M-QQEK]; *id*. ("If businesses manage to align around both the ESG mandate and their customer experience strategy, they should be able to realize significant synergies and pass the benefits on to consumers.").

107. *Id*. at VII.

108. *Id*. at 13, fig. 1. Strikingly, 56% of merchants reported that "[c]ustomer loyalty strongly influenced" their decisions in how to use data, *id*. Thus, it is not surprising why 64% of merchants indicated an increased investment in both privacy and data protection, *id*.

109. *See* Khan & Pozen, *supra* note 3, at 509 ("One way to understand this formulation is as an effort to elicit better behavior from digital companies without undermining the shareholder primacy norm . . . Delaware law would remain unaffected. The interests of shareholders would still come first." (footnote omitted)).

110. *See* Lund & Pollman, *supra* note 104, at 2615 (2021) ("As a sign of the general acceptance of value-enhancing ESG, consider that during the 2019 proxy season, more than half of the shareholder proposals brought involved ESG issues, including topics such as disclosing climate change risk and increasing board diversity."); *see generally* Larry E. Ribstein, *Fencing and Fiduciary Duties*, 91 B.U. L. REV. 899 (2011).

Additionally, Khan and Pozen argue that "the legal status quo" for *information fiduciaries* poses an issue for the duty of loyalty.[111] A corporate fiduciary has a duty of loyalty that includes, amongst other things, a duty against self-dealing and usurpation of corporate opportunities.[112] Encompassed in the duty of loyalty, a corporate fiduciary is said to be charged with an obligation to act in good faith.[113] Though Khan and Pozen assert that a fiduciary duty to end-users is inconsistent with a fiduciary duty to shareholders, respectfully, I argue that this position is myopic. Consider the Business Judgement Rule, which provides a presumption of validity in decisions made by a board of directors.[114] In the context of end-users and online service providers, a corporate decision to assure both the end-user's security and confidentiality of their personal data is likely to remain consistent with the corporate fiduciary obligation. Thus, I find Khan and Pozen's assertion that the fiduciary model is inherently beset by internal tensions to be a false alarm. Ultimately, a corporation acting as an online service provider

111. Khan & Pozen, *supra* note 3, at 503; *see id.* at 504 ("[T]hese observations give reason to question the feasibility, if not also the coherence, of applying the information-fiduciary idea to the leading social media companies. A fiduciary with sharply opposed loyalties teeters on the edge of contradiction . . . . [and] these companies may be put in the untenable position of having to violate their fiduciary duties (to stockholders) under Delaware law in order to fulfill their fiduciary duties (to end users)" (footnote omitted)).

112. *See* Julian Velasco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 66 ("The duty of loyalty plays a prominent role in corporate law. Managers are required to pursue the interests of the corporation, rather than their own interests or the interests of third parties.").

113. There is some uncertainty as to whether a corporate fiduciary acting in good faith is an independent duty or encompassed within the duty of loyalty. *See* Andrew S. Gold, *The New Concept of Loyalty in Corporate Law*, 43 U.C. DAVIS L. REV. 457, 464 (2009). For example, "the Delaware Supreme Court [has] incorporated good faith into loyalty," *id*. *See*, *e.g*., Stone v. Ritter, 911 A.2d 362 (Del. 2006) ("[A]lthough good faith may be described colloquially as part of a 'triad' of fiduciary duties that includes the duties of care and loyalty, the obligation to act in good faith does not establish an independent fiduciary duty . . . ." (footnote omitted)).

114. *See* Velasco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 62 (quoting Aronson v. Lewis, 474 A.2d 805, 812 (Del. 1984)) ("What is the business judgment rule? According to Delaware courts, '[i]t is a presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company.'") *and* Irwin H. Warren & Bradley R. Aronstam, *Delaware's Business Judgment Rule and Varying Standards of Judicial Review*, CANADIAN INST. 3 (2007), http://www.ramllp.com/media/article/12_Canadian%20Institute%20Article.pdf [https://perma.cc/P8H4-EQYT] ("[T]he venerable 'business judgment rule' prevents courts from second-guessing the decisions of independent and disinterested directors who have acted with due care and instead places the focus on the reasonableness of a board's decision-making process (i.e., whether independent and disinterested directors fully informed themselves before taking action and acted rationally).").

will not likely be conflicted when ensuring compliance with its fiduciary duties on behalf of both shareholders and end users.

2. The Fiduciary Duty viz. Online Service Providers and End-Users Should Not Belong in the Realm of Fiduciary Law, for the Analogy with Professionals is Unconvincing

Khan and Pozen's second concern is Balkin's "constructed vulnerability" in explaining the purported fiduciary relationship an online service provider exerts over an end-user.[115] Addressing an online service providers' purported expertise, Khan and Pozen point out that this "expertise may vary . . . . [and] [e]xpertise underwrites commercial fiduciary law only insofar as it enables specialized, individual judgements and services to be rendered on the beneficiary's behalf."[116] Moreover, the duo analogizes online service providers' services as "a twenty-first-century version of the Yellow Pages coupled with a communications infrastructure . . . [which is] not the kind of expertise that ha[d] helped justify fiduciary relationships in the past."[117]

I agree with the duo to a certain extent, particularly given the fact that Balkin has not sufficiently justified his two-step thesis. However, considering the *ad hoc* fiduciary relationship argument, which I proposed in Part II.a.iv, I contend that the law governing online service providers should nevertheless remain guarded by the bastion of fiduciary law. Indeed, as I have made clear throughout my argument, the digital world of online service providers has experienced a radical re-jig. Facebook has evolved from being just a social network. Even for online services such as Google or Amazon, potentially sensitive information, such as specific consumer preferences or personal search trends, may leak from Pandora's box.[118] Thus, Khan and Pozen's assertion that online service providers are

115. Khan & Pozen, *supra* note 3, at 516; *see id*. ("Balkin suggests that end users' relationships with online platforms involve a similar combination of (1) valuable expertise and (2) personal exposure necessary to enlist that expertise.").

116. *Id.*

117. *See id*. at 517; *see id*. ("Unlike in the case of obtaining legal advice or medical care, the sharing of intimate personal information with the provider is not a functional prerequisite to accessing Facebook or any other social media network.").

118. If Facebook's Metaverse comes to light, a range of biometric data extending beyond that of a "Yellow Pages" will be collected, including such things as a facial recognition algorithm. *See* Ben Egliston & Marcus Carter, *Critical Questions for Facebook's Virtual Reality: Data, Power, and the Metaverse*, 10(4) INT. POL'Y REV. 1 (2021), https://policyreview.info/pdf/policyreview-2021-4-1610.pdf [https://perma.cc/YA7C-F5G4].

merely a "twenty-first-century version of the Yellow Pages" is nothing but myopic.[119]

Additionally, the duo points out that end-users are not exposing themselves in a manner similar to other traditional fiduciary relationships, reducing end-users' need to rely on the online service providers.[120] Further, Khan and Pozen focus on online service providers' market position, arguing that "[t]o the extent that users feel beholden to Facebook, it is not because the company offers them especially skillful services or judgments so much as because of a lack of viable alternatives."[121]

Once again, I disagree. Online service providers are increasingly placing an emphasis on data protection as a core part of their business. Moreover, as companies expand the interactive suite of services that they offer to their end-users, there is an increasing trend of companies seeking to collect more than just basic personal information.[122] Take corporations operating dating apps such as Tinder, or even corporations operating convenience apps such as Uber. The former collects sensitive personal information such as personal health data (smoking habits, height, and the like) and the latter collects information such as geolocation.[123] Further, the duo downplays the striking implication of online services providers' that are increasingly requiring data collection as a pre-requisite to use their services. Here, a power asymmetry likely justifies a fiduciary relationship in this context.[124] Simply put, end-users are becoming increasingly more vulnerable in the light of growing predatory data practices by online service providers.

Substantively, I have shown that Khan and Pozen's assertion against a fiduciary relationship is weak. The duo asserts that formatively, "a fiduciary framework paints a false portrait of the digital world."[125] Here,

119. Khan & Pozen, *supra* note 3, at 517.

120. *Id.*

121. Khan & Pozen, *supra* note 3, at 518.

122. *See* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (Feb. 21, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/EHW2-YHAQ].

123. *See* Rebecca Heilweil, *Tinder May Not Get You a Date. It Will Get Your Data*, VOX (Feb. 14, 2020, 1:50PM), https://www.vox.com/recode/2020/2/14/21137096/how-tinder-matches-work-algorithm-grindr-bumble-hinge-algorithms [https://perma.cc/7JQP-W5P4] *and* Prableen Bajpai, *How Uber Uses Your Ride Data*, INVESTOPEDIA (Sept. 20, 2021), https://www.investopedia.com/articles/investing/030916/how-uber-uses-its-data-bank.asp [https://perma.cc/7TWC-2KCC].

124. *See* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2, at 1183, 1216.

125. Pozen & Khan, *supra* note 3, at 534.

the duo notes that such a framework would wrongly "characterize[] [online service providers] as fundamentally trustworthy actors who put their users' interests first."[126] Once again, I do not agree. The whole point of labeling such online service providers as "fiduciaries" is to *in fact* to counter this frequent betrayal of trust from such entities, while imbuing end-users with a greater range of tools to remedy said betrayal.[127] Further, individuals still remain autonomous, and alerting end-users that online service providers would be subject to higher duties of stewardship upon receiving one's personal data.[128] Khan and Pozen argue that a label as a fiduciary has *signaling* effects to end-users, yet I could very well argue the same in reverse.[129] Making online service providers aware that they may incur liability under fiduciary law would likely prompt a re-jig of their own business practices considering that providers are subject to higher duties.

I acknowledge that difficult facts may make difficult cases. But as made clear in my arguments earlier, just because there is resistance against such reforms in the law does not mean that no reform should be taken. This is but a repeat reprisal of an argument once advanced in the 1930s financial markets. At that time, the stock market crash in 1929 was in part fueled by a thriving host of misinformation created because of inadequate disclosures and misleading promises of large profits from companies to investors, which lacked substantive basis, with some even being wholly fraudulent.[130] In its aftermath, a speculative sell-off frenzy resulted, which decimated the stock market. This led to Congress passing the Securities Act of 1933, ensuring more transparency in financial statements so that investors could make more informed decisions, as well as creating liability for misrepresentation and fraud in the securities market.[131]

Dissenters to the Act may argue that misleading investors in the stock market is a practice that is heavily imbued in the business model of the sale of securities, and that without such practices selling securities and raising capital would simply be impossible. Otiose as this may seem, this is exactly what Khan and Pozen have been arguing. Here, we are seeking to impose a fiduciary relationship in precisely *such* a case because even

126. *Id.*

127. *See generally* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 2.

128. *See* Khan & Pozen, *supra* note 3, at 508.

129. *See id*. at 534-35.

130. *See id*. at 521, 535.

131. *See generally* Securities Act of 1933, 15 U.S.C. § 77a.

for businesses focused on "behaviorally targeted advertising," it has already been shown that they are not trusty data stewards.[132] Imposing a fiduciary relationship would implore online service providers to seek a re-jig in their business model, ushering in a new era of responsible data practices. Thus, I have shown that Khan and Pozen's siege against the existence argument cuts little ice and should not be viewed as any deterrence against a fiduciary model in the context of online service providers. Though I agree that Balkin's thesis is flawed, Balkin's fault is limited to a lack of justification for holding online service providers accountable. This can be solved by the *ad hoc* doctrine proposed in this Article.

3. Is This the End for Targeted Advertising?

Though generally addressed the thrust of Khan and Pozen's argument, it remains helpful to knock off any remaining specific dissent pertaining to this concern. According to the duo, the imposition of fiduciary duties on online service providers spells the end for targeted advertising as providers generate significant revenue from such advertising.[133] Under such a duty, online service providers are forced to constantly labor under a "profound and 'perpetual' conflict," placing the online service provider's economic interests directly at odds with their end-users.[134] Therefore, the fiduciary model will decimate the industry and sits uneasily with the core tenets of fiduciary law itself.[135]

Respectfully, I think that the duo goes a step too far because their idea rests on the erroneous assumption that all targeted advertising is abusive as well as that such advertising sits uneasily against the fundamental interests of its beneficiaries. Ever since the advent of the fourth industrial revolution, much scholastic effort has been conducted on this topic. Minh-Dung Tran, for example, suggests a "novel design" for targeted advertising technology, especially if online service providers latch onto a "privacy-by-design targeted advertising model which allows personalizing ads to users without the necessity of tracking."[136] Here, Tran suggests such "retargeting advertising" would sufficiently provide

132. Khan & Pozen, *supra* note 3, at 515.

133. *Id.* at 512, 516 ("[Online service providers] will be economically motivated to extract as much data from their users as they can—a motivation that runs headfirst into users' privacy interests as well as any interests users might have in exercising behavioral autonomy.").

134. *Id.* at 513.

135. *See id.*

136. Minh-Dung Tran, Privacy Challenges in Online Targeted Advertising, i, 101 (Nov. 13, 2014) (Ph.D. dissertation, University of Grenoble) (HAL).

"strong user privacy while still ensuring ad targeting performance and being practically deployable."[137]

Similarly, Leslie John et al. have heralded a trifurcated approach to create targeted advertising, utilizing the factors of trust, control, and justification to support their approach.[138] For trust, the study highlighted "voluntary ad transparency" as one way to reduce the possibility of abusive advertising.[139] Here, the study noted that high trust in the provider in conjunction with ad transparency actually increases "click-through rates."[140] Ultimately, the study reported that informing end-users of targeted advertising on the site increased click rates, the time spent viewing products and the revenue ultimately generated.[141] Per control, the study highlighted end-users "[do] not object to information being used in a particular context, but they worry about their inability to dictate who else might get access to it and how it will be used down the line."[142] The authors noted that "when consumers are given greater say over what happens with the information they've consciously shared, transparently incorporating [targeted advertising] can actually increase ad performance."[143] For justification, the report argued that "[r]evealing why personal data has been used to generate ads can help consumers realize the upside of targeted ads."[144] The authors further noted that "[[i]f [online service providers] have difficulty coming up with a good reason for the way [they] use consumers' data, it should give [them] pause."[145] These three factors, taken together, once again suggests that Khan and Pozen's view is myopic. Acting in the best interests of end-users will not, even in

137. *Id.* at i.

138. *See* Leslie K. John et al., *Ads That Don't Overstep*, HARV. BUS. REV., Jan.-Feb., 2018.

139. *Id.* at 6.

140. *Id.* ("Many now display an AdChoices icon, a blue symbol indicating that the accompanying ad has been tailored to the individual recipient's characteristics.").

141. *Id.* at 6-7 ("[W]hen we revealed first-party sharing by telling shoppers that an advertisement was based on their activity on the site, click-through rates increased by 11%, the time spent viewing the advertised product rose by 34%, and revenue from the product grew by 38%.").

142. *Id.* at 7.

143. *Id.* at 8. The cited study looked at ad engagement with an attribute that a user had previously revealed. At the study's midpoint, the online service provider changed their privacy policy, which allowed end-users to "manage their privacy settings more easily," *id.* at 7. The study showed that "[a]fter the change, however, the personalized ads were almost twice as effective as the generic ones," *id.* at 7-8.

144. *Id.* at 8.

145. *Id.*; *see id.* ("In one experiment . . . a personalized ad by a movie rental company that invoked users' physical locations backfired, but its performance improved when the copy explained why the physical location was important: The consumer was eligible for a service not available in all places.").

the targeted advertising context, reduce profitability, nor lead to a breach of fiduciary duties to online service providers' stockholders. Rather than targeted advertising creating a binary conflict, John et al. show that targeted advertising can act in the interest of end-users and benefit businesses simultaneously.[146] Further, using fiduciary obligations to limit abusive practices by targeted advertising would force offending organizations to instead adopt an approach as suggested by the above study, leading to a business ecosystem that respects sanctity of personal data.

C. The Scope of Fiduciary Duties of An Online Service Provider as an Ad Hoc Fiduciary

One question remains to be answered, about *how* should we craft the scope of duties for online service providers that are held to be fiduciaries. As a starting principle, "a fiduciary duty extends to every possible case in which there is confidence reposed on one side and the resulting superiority and influence on the other; the rule embraces both technical fiduciary relations and those informal relations which exist whenever one person trusts in and relies upon another."[147] Kelly highlights that the duty of loyalty and care typical in an *ad hoc* case is largely analogous to the standard as applied in a *status-based* case.[148] The nub of the issue therefore centers on what duties apply in the online service provider context.

1. The Duty of Loyalty

The first duty undergirding the proposed fiduciary model is the duty of loyalty.[149] Kelly states that the duty of loyalty is "similar to loyalty principles from the categorical fiduciary fields," and applies with full

146. *See id*.

147. 37 AM. JUR. 2D, *Fraud and Deceit* § 35, 1-2 (2018) (footnote omitted).

148. *See* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35; *see also* Janice D. Villiers, *Clergy Malpractice Revisited: Liability for Sexual Misconduct in the Counseling Relationship*, 74 DENV. U. L. REV. 1, 21 (1996).

149. *See generally* Villiers, *supra* note 148. The complementary duty, the duty of care, likely also undergirds the proposed model. For *ad hoc* fiduciaries, US jurisprudence has suggested that duty of care principles apply in a similar manner to that fashioned in the *status-based* case law. *See, e.g*., Benjamin v. Kim, No. 95 CIV. 9597 (LMM), 1999 WL 249706, at 8 (S.D.N.Y. Apr. 28, 1999); Mountcastle v. Baird, No. CA 33, 1998 WL 5682, at *3 (Tenn. Ct. App. Jan. 29, 1988).

force.[150] For example, the Federal Circuit has concluded university educators as "liable for breaches of their fiduciary duty based . . . on their blatant pursuit of self-interest at the great expense of trusting students."[151] Though the degree of "the duty of loyalty does vary in accordance with the varied applications," it is undeniable that such a duty sit "at the heart of all fiduciary relationships."[152]

Paul Miller and Andrew Gold describe the two accounts underpinning the traditional notion as to the whom the duty of loyalty extends as "proscriptive accounts and prescriptive accounts."[153] Here, Miller and Gold note that "[p]roscriptive accounts focus on the types of conduct that fiduciaries are prohibited from participating in."[154] Under proscriptive accounts, the duo describe a fiduciary's obligations as encompassing "the two so-called conflict rules," the conflict of interest rule and the conflict of duty rule.[155] Using this as a basis, Richard Whitt described the conflict rules as the "'thin' version" of the duty of loyalty, representing "a technical, state-enforced obligation."[156]

By contrast, "[p]rescriptive accounts . . . suggest that the fiduciary must demonstrate her loyalty through some affirmative conduct."[157] Under prescriptive accounts, Miller and Gold describe a fiduciary's obligation which "requires that one take initiative to benefit one's

150. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 14 (footnote omitted).

151. Rebekah Ryan Clark, Comment, *The Writing on the Wall: The Potential Liability of Mediators as Fiduciaries*, 2006(4) B.Y.U. L. REV. 1033, 1039 (2006) (citing Chou v. Univ. of Chi., 254 F.3d 1347, 1362 (Fed. Cir. 2001)).

152. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 14 (footnote omitted). When the duty of loyalty has been applied in disparate ways, scholars typically note that such differences stem from differing evidentiary requirements imposed by state courts, *see id*.; *see also* Gregory B. Westfall, *But I Know It When I See It: A Practical Framework for Analysis and Argument of Informal Fiduciary Relationships*, 23 TEX. TECH. L. REV. 835, 837 (1992).

153. Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM & MARY L. REV. 513, 556 (2015); *id*. ("Most accounts of the [fiduciary] duty [of loyalty] assume that it is directed towards a person or persons who enjoy a corresponding claim right to the fiduciary's loyalty.").

154. *Id*.

155. Paul B. Miller, *A Theory of Fiduciary Liability*, 56(2) MCGILL L.J. 237, 257 (2011) ("First is the requirement that the fiduciary avoid conflicts between pursuit of his self-interest and fulfilment of his duty to act for the benefit of the beneficiary (the conflict of interest rule). Second is the requirement that the fiduciary avoid conflicts between this duty and the pursuit of others' interests (the conflict of duty rule).").

156. Richard Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75, 93 n.105 (2020).

157. Miller & Gold, *Fiduciary Governance*, *supra* note 158, at 556-57.

beneficiary."[158] Richard Witt notes that "the duty of loyalty [often] goes beyond its proscriptive foundation . . . [and] is combined with [related duties] to create a prescriptive obligation to act in the best interests of the beneficiary."[159] Here, Whitt views a fiduciary's obligation of acting in the beneficiary's "best interests as the thick version of loyalty, impl[ying] a specific emotional and intellectual orientation of selflessness towards one's principals."[160]

How might the concepts of think and thick loyalty play out in the context of online service providers? As noted in Part II.b.i, dissenters have argued that the fiduciary model is inherently beset by internal tensions. Per the *conflict of duty* element, fiduciaries must not pursue interests for beneficiaries when these interests are inherently conflicted. However, as I have demonstrated in Part II.b.i, the duties to end-users are not inherently conflicted with duties to stockholders, and it is likely that the duty of loyalty is not breached.

Pertaining to the content and intensity to be applied, it is unlikely such a duty should be subject to any requirement for "informed consent." Indeed, regarding the intensity of the duty of loyalty, Neil Richards and Woodrow Hartzog's thesis provides a good starting point.[161] These scholars make a relevant salient argument that "[o]ne of the most important traits of U.S. data privacy law and data protection regimes around the world is that they rarely differentiate between large, powerful organizations and small, weaker ones."[162] Yet, Richards and Hartzog are quick to note that "there is a world of difference between Facebook and your local coffee shop."[163] Recognizing that the power dynamic embedded within privacy law,[164] they argue that "the obligations of loyalty owed by companies should be roughly proportional to the amount of power they have over people."[165]

I argue that Richards and Hartzog's thesis is consistent with the *ad hoc* fiduciary approach advanced in this Article. For example, Richards

158. *Id.*

159. Whitt, *supra* note 156, at 93.

160. *Id.* at 93 n.105.

161. *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021).

162. *Id.* at 1008.

163. *Id.* at 1008-09.

164. *See id.* at 1009 ("Privacy law is about power, and privacy law should be sensitive to the contexts in which that power is amassed and used." (footnotes omitted)).

165. *Id.* (footnote omitted). Richards and Hartzog suggest several power metrics that could be used, "including market power, time spent using the service, amount of data collected, the nature of the data collected, degree of vulnerability, and the function of the service offered," *id.*

and Hartzog suggest that online service platforms should be grouped be considered as "business in the top tier,"[166] and thus be subject to more regulation.[167] Further, Richards and Hartzog would subject such companies with "a general relational duty of loyalty owed to those who entrust these companies with their data and online experiences."[168] Earlier, I argued that such changes are not inherently bad and may in fact resonate with modern business practices. Through an *ad hoc* based rationalization, courts may likewise use the above-suggested criterion by Richards and Hertzog in determining the intensity of the duty of loyalty, which will ultimately prompt a re-jig in business practices towards an ecosystem that respects the personal data of end-users better.

2. The Duty of Care

Relatedly, a duty of care exists in a fiduciary law. Similar to duties of care in other areas of law, a "party who exercises a sufficient degree of care is relieved of liability."[169] However, in a fiduciary law context, the duty of care "creates an additional objective standard, one of ordinary care, prudence, and diligence by a party with particular knowledge or skills carrying out its assigned duties."[170] Some scholars view the consideration of a party's knowledge or skill to modify the standard of liability, where "a fiduciary duty of care can be breached by an entity's mis-performance, even absent any injury to the beneficiary."[171] Importantly, "[t]he content of the duty of care can be highly contextual," applying varying levels of liability depending on the applicable area of law.[172]

166. *Id*. The duo describes top tier businesses as "those with the most power over people using their services due to their exposure and, consequently, the highest risk for opportunism," *id*.

167. *Id*. ("One idea could be to look to whether a company requires a user to create an account and log in to use its service. This would be evidence of looking to create a more lasting information relationship than a single transaction.").

168. *Id*. Richards and Hartzog provide a range of measures that would impose a general duty of loyalty, which "would include specific prohibitions on conflicted design and data processing, invalidation of attempted waivers, disclosure requirements, and the full suite of rebuttable presumptions against specific kinds of disloyal activities," *id*.

169. Whitt, *supra* note 161, at 91.

170. *Id*. at 92. (footnote omitted).

171. *Id*. (footnote omitted); *see* John C.P. Goldberg, *The Fiduciary Duty of Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 408 ("[T]he breach of a fiduciary duty of care can generate liability—i.e., a change in legal relations- even if the breach does not result in injury.").

172. Whitt, *supra* note 156, at 92 ("For example, the obligation can be quite lax as applied in corporate law (shielded in part by the business judgement rule), while highly stringent in trust law (amounting to a relatively strict standard of prudence)." (footnote omitted)); *see also* Hanoch

Balkin has addressed the duty of care in his information fiduciary model, utilizing Facebook's Cambridge Analytica scandal to illustrate this duty.[173] As a threshold matter, Balkin notes that "a digital company has a duty to protect its end-users not merely from its own actions, but also from the actions of those with whom it shares data."[174] Here, Facebook failed its duty of care by "not vet[ting] its contractual partners . . . [and by failing to] make sure that it shared end-user data only with trustworthy persons and companies."[175] The content of the fiduciary duty of care for online service providers should, therefore, depend on the business judgment rule, and as a result, the intensity is likely to be rather lax. Most online service providers should not breach this duty unless they have implemented such otiose data protection practices to the extent that one can hardly say that this is in the interests of any ESG concerns.

3. The Subsidiary Obligations

Amongst other obligations constructed by the court, the duty of confidentiality is probably most relevant to online service providers.[176] Though there is no bright line test for determining whether a duty of confidentiality arises on the facts, Giles suggest that courts should take into account "the length of time of the reliance, a disparity in the positions of the parties, and a close relationship between the parties."[177] The proposed model of this Article likely gives rise to a relationship with sufficient "evidence of a confidential relation."[178]

Dagan & Sharon Hannes, *Managing Our Money: The Law of Financial Fiduciaries as a Private Law*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 99 (2014).

173. Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66(5) BUFFALO L. REV. 979, 1009 (2018).

174. *Id.* at 1008 ("The duties of care and confidentiality require information fiduciaries to keep data secure and not to disclose it to third parties unless those third parties are equally trustworthy and agree to the same duties of care, confidentiality, and loyalty as the fiduciary." (footnote omitted)).

175. *Id.* ("In short, the Cambridge Analytica scandal demonstrated most of the things that an information fiduciary should *not* do with its end-users' data.").

176. *See also* Roy Ryden Anderson, *The Wolf at the Campfire: Understanding Confidential Relationships*, 53 S.M.U. L. REV. 315, 317 (2000) ("[C]onfidential relationships have been labeled 'fact-based' fiduciary relationships to distinguish them from formal [fiduciary relationships]." (footnote omitted)); *see generally* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35.

177. Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 41 (1995) (footnote omitted).

178. *Id.* (footnote omitted). Here, the evidence would include "great intimacy, disclosure of secrets, entrusting of power, and superiority of position," *id*.

Relatedly, Sitkoff notes that "*subsidiary* or *implementing* fiduciary duties, are typically structured as *rules* or at least as *more specific standards* that speak with great specificity."[179] However, the advocated *ad hoc* proposal might pose problems for implementing the duty of confidentiality. Here, Sitkoff notes that the proposed model of "[f]act-based fiduciary relationships recognized ad hoc" may encounter difficulty as such a "model . . . presumes recurring circumstances within a specific type or kind of fiduciary relationship."[180] As an *ad hoc* rationalization, it may be contended that the subsidiary duty of confidentiality cannot apply. Nevertheless, Sitkoff's second mode of escape may prove to be the most salient, in which Sitkoff contends that "there might be recurring facts and circumstances in certain recurring forms of fact-based fiduciary relationships such that courts might develop subsidiary fiduciary duties for those cases."[181] This solution may be viable because end-users, as argued in Part I.a.iii, are often in a relationship of vulnerability to online service providers, which leads them to repose trust and confidence when providing their personal data.

The duty of disclosure is likely in play as well. As Palmieri notes, "[t]he courts, in effect, have been able to impose a duty of full disclosure of material facts during negotiations on an *ad hoc* basis by labeling a relationship as confidential or fiduciary in nature."[182] Andrew Tuch, looking instead to banking law, has noted that "the duty of disclosure may put a bank in the position of owing conflicting duties . . . [yet] [t]his risk has not stopped courts from imposing a duty of disclosure."[183] It is not too much of a leap to therefore hold the duty of disclosure as relevant for online service providers as well.

Importantly, Kelly has noted that "the duty of disclosure generally does not apply to parties in an arm's-length transaction."[184] Here, Kelly

179. Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 419.

180. *Id.* at 433.

181. *Id.* Sitkoff also posits another solution: in "courts might draw by analogy on subsidiary fiduciary duties from the categorical fiduciary fields, just as similar fiduciary duties are found across fiduciary categories with similar circumstances," *id*.

182. Nicola W. Palmieri, *Good Faith Disclosures Required During Precontractual Negotiations*, 24 SETON HALL L. REV. 70, 128-29 (1993) (footnote omitted).

183. Andrew F. Tuch, *Fiduciary Principles in Banking Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 129.

184. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 17. Arm's length transactions have been described as "the purchase and sale of a business [when] invol[ing] intelligent, capable businessmen, who are represented frequently by counsel and/or experts," Palmieri, *supra* note 182, at 181.

notes that "liability may turn on whether a court concludes that parties in a transaction are in a fact-based fiduciary relationship or in an arm's-length transaction."[185]

A careful analysis of the common law of disclosures reveals that, regardless of the contractual transaction involved, the unifying principle behind required disclosures is the dictate of good faith and fair dealing . . . A duty of good faith and fair dealing applies whether there is a contract or not, and therefore also applies to precontractual negotiations as well as to contract performance.[186] Ultimately, whether a duty of disclosure arises will likely depend on whether the data transaction between the parties is an *ad hoc* or arm's length transaction.[187] As argued in this Article, this is often the former, because of the information asymmetry coupled with ambiguous data protection policies. Therefore, a duty of disclosure the extent to which personal data will be used is likely present on such a model.

D. Remedies and Conclusion

Having crafted together a workable *ad hoc* model that links online service providers and end-users, end-users would be permitted to the full suite of remedies offered by a breach of fiduciary duty. Courts have emphasized that the "same remedy" that are relevant to a breach of trust applies likewise for "both technical and fiduciary relations, and those informal relations which exist whenever one man trusts in and relies on another."[188] Further, an end-user may advance a claim for the traditional equitable remedies, ranging from equitable compensation to an account for profits as well as for a constructive trust.[189] Notably, the remedy of equitable compensation may play a larger part in supporting an *ad hoc* fiduciary rationalization.[190] Here, Jeff Berryman notes that "[e]quitable

185. Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 17.

186. Palmieri, *supra* note 182, at 75.

187. *Id.* at 129.

188. *See e.g.*, Dick v. Albers, 90 N.E. 683, 684-685 (Ill. 1909); Fitz-Gerald v. Hull, 237 S.W.2d 256 (Tex. 1951).

189. Some scholars have argued that data subjects should be protected with "consumer protection rules." *See* Gianclaudio Malgieri, *Property and (Intellectual) Ownership of Consumer's Information: A New Taxonomy for Personal Data*, 2016(4) PING 133, 138 (2016).

190. *See also* Jeff Berryman, *Fact-Based Fiduciary Duties and Breaches of Confidence: An Overview of Their Imposition and Remedies for Breach*, 37 NZBLQ 95 (2009) ("As the nomenclature implies, equitable compensation is a compensatory remedy and thus only achieves disgorgement as a secondary consequence, and then only if is useful to measure the innocent party's actual losses.").

compensation has increased in importance as a consequence of the fact that larger spheres of human conduct operate in areas that have traditionally invoked equity's substantive jurisdiction, namely fiduciary duties (particularly the expansion of fact-based fiduciaries) and confidences."[191]

Thus far, I have argued that an *ad hoc* fiduciary rationalization between online service providers and end-users is the preferable model to imbue the end-users with a *bottom-up* workable enforcement mechanism that would possess some teeth in the United States. This has caused me to diverge from Balkin's seminal *information fiduciary* thesis, wherein Balkin views *information fiduciaries* as a *status-based* fiduciary relationship.[192] Further, I have addressed the major dissent to Balkin's model, put forth by Khan and Pozen. There, I noted formative and substantive issues with the duo's attempt to defeat a fiduciary rationalization. Finally, I rationalized the envisioned scope of duties governing an *ad hoc* rationalization, which would include a strong duty of loyalty and a slightly weaker duty of care, supported by subsidiary duties of confidentiality, good-faith, and disclosure.

III. A TRADITIONAL TRUSTS-BASED RIPOSTE FOR ENGLISH LAW?

The most developed rationalization undergirding the traditional trusts-based camp finds itself in Delacroix and Lawrence's paper.[193] Hitherto, the primer of this Part will be divided into two sections. In the first, I address and counter the Delacroix and Lawrence's repartee against Balkin's *information fiduciary* model, but more importantly, I prove the duo's concerns as otiose, particularly against the proposed model in this paper. In the second, I canvas Delacroix and Lawrence's proposed traditional trusts-based rationalization through examining its merits in the context of English law. In the final analysis, I show that this Article's proposed fiduciary model presents a far more flexible approach against the proposed data trust strategy for English law, as the latter simply opens a can of worms.

A. The Counterattack Against a Fiduciary Model

Delacroix and Lawrence's main contention against a fiduciary rationalization centers on the fact that it "does not tackle the power

191. *Id.*

192. As discussed, a *status-based* rationalization is inappropriate as this herald rigid *scope* issues due to the myopic application of a blanket rule.

193. *See generally* Delacroix & Lawrence, *supra* note 9.

asymmetries inherent in our current system of data feudalism."[194] The duo points out that in cases where a "data controller has . . . data provided by data subjects, this results in a conflict between that interest and her duty towards data subjects."[195] According to them, "[d]ata controllers in this position would be obliged to both maximize the value of the personal data they collect (for the benefit of shareholders) and concomitantly honour fiduciary obligations towards data subjects."[196] Therefore, they assert that a fiduciary rationalization "fails to draw the only logical conclusion: a fiduciary obligation towards data subjects is incompatible with the data controllers' responsibility towards shareholders."[197] This is because "honour[ing] a fiduciary obligation not only demands independence from profit maximization . . . [but also] an ability to relate to the complex and multi-faceted nature of vulnerability inherent in the data subject/data controller relationship," with Balkin's model being akin to a "doctor who gains a commission on a particular drug prescription or a lawyer who uses a company to provide medical reports for his clients while owning shares in the company."[198]

However, I contest that Delacroix and Lawrence's repartee is nothing but blunt. The duo's claim that "[d]ata controllers . . . would be obliged to maximize the value of the personal data they collected (for the benefit of shareholders)" does not account for the existence of other business judgment considerations such as ESG.[199] Hitherto, Delacroix and Lawrence's counter-attack tumbles into a similar lacuna as that of Khan and Pozen, therefore rendering the fiduciary model unscathed.

Delacroix and Lawrence's second contention is that "Balkin's information fiduciary proposal only affords protection to those who are already in a contractual relationship with 'digital companies.'"[200] Here, the duo asserts that this presents a problem for Balkin's *status-based* categorization, as Balkin has acknowledged that "there are a wide range of situations in which people lack a contractual relationship with a digital enterprise or with a business that collects personal information and uses algorithms to make decisions."[201] To address "concepts of public and

194. *Id.* at 241.
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.* at 241-42.
199. *Id.* at 241.
200. *Id.* at 242.
201. Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51(3) U.C. DAVIS L. REV. 1149, 1163 (2018).

private nuisance," the duo further maintains that given "the nature of the 'nuisance' at stake, the remedy proposed by Balkin is puzzling."[202]

I, however, contend that Balkin's attempted rationalization via a public/private nuisance analogy heralds nothing but a leap out of the frying pan into the fire. Respectfully, utilizing a nuisance-based model engenders difficult issues of quantification. As Declaroix and Lawrence have pointed out, it remains difficult to even quantify the underlying "social costs" that companies have "shifted onto others."[203] Thus, this Article contends that a nuisance approach is likely an incorrect turn.

Keith Hylton, taking a different approach, views the "building blocks of [the United States'] theory of nuisance doctrine" as "the economic model of strict liability."[204] Hylton illustrated that "strict liability has the property that it imposes liability on actors even when they have taken reasonable care."[205] This becomes clear if one examines how a private individual evaluates his privately optimal level, which is the point wherein he maximizes his utility for the given activity. Hylton described a point where the marginal private benefit (MPB) intersects to the private actor intersects with the marginal private cost, creating a point at which the private individual's privately optimal activity would be chosen. Applying Balkin's model then onto Hylton's framework, Balkin claims that "[u]sing algorithms repeatedly and pervasively over large populations of people may inappropriately treat people as risky or otherwise undesirable, impose unjustified burdens and hardships on populations, and reinforce existing inequalities."[206] The negative externality is therefore incurred as "unjustified burdens and hardships."[207]

Hylton further discussed instances when a nuisance strategy might be apt.[208] Here, Hylton suggests the conclusion one may draw from these use cases is "strict liability is desirable in the single activity case only when the external costs of the activity substantially exceed the external benefit associated with the activity."[209] In such a case, imposing strict

202. Delacroix & Lawrence, *supra* note 9, at 242; *see* Balkin, *Free Speech in the Algorithmic Society*, *supra* note 201, at 1168 ("The appropriate remedy is to make companies internalize the costs they shift onto others and onto society as a whole as they employ algorithmic decision making.").

203. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 201, at 1168.

204. Keith N. Hylton, *The Economists of Public Nuisance Law and the New Enforcement Actions*, 18 SUP. CT. ECON. REV. 43, 47 (2010).

205. *Id.* at 52.

206. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 201, at 1167.

207. *Id.*

208. *See* Hylton, *supra* note 204, at 53.

209. *Id.*

liability "reduces activity levels to a point that is closer to the socially optimal scale than would be observed under the negligence rule."[210] Indeed, if "the external benefits are roughly equal to or greater than the social costs associated with the activity, strict liability is not [likely] socially desirable."[211] Therefore, the question turns towards whether the external costs of using algorithms substantially exceed any external benefits associated with the activity.

Delacroix and Lawrence also point out that Balkin "fails to dwell on the process that would somehow enable the quantification (and hence 'internalization') of the 'cost' of treating people as 'otherwise undesirable.'"[212] Indeed, the duo suggest that Balkin's cost-benefit calculation is a bark up the wrong tree: the externality created is "not merely one [created from] material resources or opportunities," but instead an external cost imposed onto individuals against their "ability to maintain a social self," ultimately "undermines [an individual's] commitment to moral equality."[213] Thus, lacking an accurate or even certain way of measuring the exact external cost of using algorithms, especially at a premature stage, a nuisance approach via strict liability is therefore the less preferable choice.

Balkin does propose the nuisance theory merely as a way of stretching his *information fiduciaries* theory further—but even if this is the case, this is something we need not develop further if we adopt the *ad hoc* rationalization. I return to the factors outlined by Kelly in which an an *ad hoc* fiduciary may arise.[214] Balkin asserts that "there cannot be a fiduciary relationship—at least before a relationship is formed."[215] This is inaccurate. In most cases where individuals pass their personal information to another party to seek an opportunity, factors (i)-(iii) may still be made out. For (i), the information can be passed with some level of confidence that it will only be used for the appropriate purposes of seeking the opportunity, for (ii), individuals largely lack expertise in the big data activities such organizations do perform, and for (iii), individuals do wholeheartedly believe that such organizations will handle their data appropriately and would be willing to part with any relevant data that may give them an edge to attain the opportunity.

210. *Id.*

211. *Id.*

212. Delacroix & Lawrence, *supra* note 9, at 242.

213. *Id.*

214. *See* Kelly, *Fiduciary Principles in Fact-Based Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW, *supra* note 35, at 9.

215. Balkin, *Free Speech in the Algorithmic Society*, *supra* note 201, at 1164.

Likewise, on the other side of the fence, (i) such organizations often have *significant discretion* over the information that is handed over; whilst holding (ii) themselves out with *particular expertise, knowledge, or trustworthiness*, for they compel individuals to hand over information in order to procure an opportunity; and (iii) such organizations have all the power over said individual's personal data and therefore act in a position of *superiority* over the end-user.

Taken together, there is sufficient reason to undergird this relationship with the protective arms of fiduciary law if the above conditions are met. An *ad hoc* rationalization produces a far cleaner solution in our quest to leap over the knotweeds. This is the superior approach in U.S. law.

B. A Traditional Trusts Approach?

Moving across the Atlantic, it must be queried whether an *ad hoc* rationalization fits as neatly in English law as it does for U.S. law. As compared to U.S. law, a fiduciary approach in scholarly literature has yet to take hold, however, and it is therefore astute to examine the developed works in this area. This is arguably Delacroix and Lawrence's thesis on traditional trusts, and a deep dive into their argument supporting a traditional trusts model is therefore relevant, in a bid to examine if this proves to be the *ad hoc* fiduciary doctrine's worthy contender.

The duo's main contention is that "[t]axes and economic incentives" do not solve "structures that foster what may aptly be described as a form of social cruelty."[216] They argue a re-jig is needed from the "ground-up."[217] Compared to a focus "on compensation for the undesirable risks or side-effects that stem from the current exploitation of our data by centralized platforms," the duo argues a traditional trusts framework will "empower data subjects[] to 'take the reins' of their data."[218] In this subsection, I consider, and distinguish, this approach from the *ad hoc* rationalization. Ultimately, I riposte a traditional trusts model as *plausible* under English law. However, I continue to advance the viability of an *ad hoc* fiduciary model, for it produces a neater solution complimentary to the GDPR regime in the UK and is a "bottom-up" enforcement approach that is more in line with the duo's thesis.

216. Delacroix & Lawrence, *supra* note 9, at 242.
217. *Id.*
218. *Id.*

1. Advantages of the Present Proposal

The starting point of the duo's proposal finds an attempt to distinguish themselves from other approaches in the UK.[219] Indeed, the duo argues a "'true' Trusts" as preferable instead—for the "collective setting of terms . . . is a way for data subjects to pool their rights to acquire a 'voice," much akin to "[Freeland] Land Societies" during the early English ecosystem that sought to provide the working class empowerment to vote through the ownership of land.[220] Here, "[t]he terms of the Trust may specify a governance structure that compels data Trustees to continuously consult and deliberate with [end-users]."[221] The advantage of creating a formal relationship, according to the duo, is to establish the online service provider and end-user relationship to entitle end-users the ability to equip themselves with the protection of fiduciary law.[222]

Prima facie, this appears to be just another well-worn hat that seeks to embeds the online service provider/end-user relationship with the bastion of fiduciary law. Nevertheless, the duo argues that the merit of this approach is that the traditional trusts model is "resolutely complementary to [the] top-down, regulatory constraints" of English law and the GDPR.[223] In the development of such trusts in future jurisprudence, the duo therefore argues that support for such a model will "play an important role in shaping societal debate about" the feasibility of requiring individuals to think beyond themselves, contributing to a greater societal good.[224]

Under this new orthodoxy, the duo foresees "a wide variety of data Trusts" being set up, some "favour[ing] the furthering of some 'public good' endeavour by making some data freely accessible to some organizations, while others may prioritize the maximization of financial returns," and some fueled with the main purpose of "minimizing individual risks."[225] However, they admit that such an ecosystem is impossible unless (i) the creation of new trusts is a simple process and (ii) the security of such information stored in said trusts are assured.[226] There are certainly weaknesses to such a pronounced approach—indeed, the duo asserts that "many Trusts may prefer to focus on collectively

219. *See generally* Hall & Pesenti, *supra* note 19.
220. Delacroix & Lawrence, *supra* note 9, at 242.
221. *Id.*
222. *See also id*. at 237.
223. *Id.* at 243.
224. *Id.*
225. *Id.*
226. *Id.*

setting the terms according to which [end-users'] data may be used, relying on computational and storage infrastructure from commercial suppliers."[227] The problem arises that a new era of data trusts would require a fundamental re-jig and even an augmentation of current infrastructure, processes which necessitate a pronounced industrial effort to facilitate this new model.

Yet, other problems remain. Such a system, if set up, implies a "system of data exchange between Trusts and consumers of the data."[228] Thus, I believe it is worth examining the current legal rights accorded to individuals under the top-down framework in English law. For example, Portability is proscribed by Article 20 of the GDPR.[229] Indeed, Article 20(1) augments data subjects with the "right to receive the personal data concerning him or her, which he or she has provided to a controller."[230] However, this right is limited by Articles 20(1)(a), which requires the processing *viz*. the data controller to be given with prior consent pursuant to Article 6(1)(a) or pursuant to a contract per Article 9(2)(a). This straddles uneasily with the Right of Access embedded in the GDPR,[231] because although the Right of Access permits the data subject "the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed."[232] The data, when requested, "shall be provided in a commonly used electronic form."[233] On the ambit of erasure, Article 17 grants the data subject the ability to request erasure only in six specific circumstances. Yet, Article 17(3) provides times when the right of erasure "shall not apply to the extent that processing is necessary."[234]

Taken together, the present legal framework of data protection is unequipped to herald in an era of traditional data trusts. Even with portability and access rights, said measures will only be effective insofar as access rights are instantaneously given. Presently, under the GDPR, organizations are mandated to respond to data access requests within one month.[235] However, for a data trust to work, it is likely that the rights of

227. *Id.*
228. *Id.*
229. Council Regulation 2016/679, art. 20, 2016 O.J. (L 119), 38 (EU) [hereinafter GDPR].
230. *Id.* art. 20(1).
231. *See id.* art. 15(1).
232. *Id.*
233. *Id.* art. 15(3).
234. *Id.* art. 17(3).
235. *See Right of Access*, INFORMATION COMMISSIONER'S OFFICE [ICO] (2022), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ [https://perma.cc/XH96-WLGS].

portability, erasure, and access must be almost instantaneous. Recital 63 of GDPR is relevant, which states that "[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data."[236]

Nevertheless, supporters of the traditional trusts approach may contend that developing data trusts as an *opt-in* model encourages a tradition of strong data compliance practices going forward. I agree that a fundamental re-jig would be prompted by the traditional approach, and therefore a traditional trusts approach is plausible, and perhaps even with its merits. In the next subsection, I continue to address two further dissents on issues relevant to property and relevance that plague the traditional trusts rationalization. By defending the traditional trusts approach and comparing it against this Articles's *ad hoc* model, one may likely come towards a more convincing conclusion as to why the *ad hoc* rationalization is far more preferable.

2. Justifying a Traditional Trusts Framework

Dissenters to the traditional trusts approach in English law are likely to cite the ODI report which I referenced in Part I of this Article. Indeed, the ODI report claims that "data is not capable of constituting property in the legal trust sense, and thus cannot form the basis of a legal trust in any of the legal systems which have a concept of trust law."[237] There have also been contentions that shared provenance issues arising from the lack of identifiability of data, alongside questions on assignability, which stand as a bastion against this model's success.[238] Furthermore, it has been argued by the ODI that data trusts will only be relevant only for a small number of data trusts, which I call the "relevance" quandary.[239] I address both contentions below, ultimately concluding they can be resolved, albeit uneasily.

a. The Property Problem

The central problem finds itself in the ability of information as rights to be held under a trust. Delacroix and Lawrence attempt to deduce the intentions of the ODI report, asserting that the ODI may have been

236. GDPR, *supra* note 229, Recital 63.

237. Reed, *What is a Data Trust in Legal Terms?*, *in* DATA TRUSTS: LEGAL AND GOVERNANCE CONSIDERATIONS, *supra* note 28, at 12.

238. *Id.*

239. *Id.*

referring to the fact that "data is an intangible asset."[240] However, Sarah Worthington has made clear that the bifurcation between tangible and intangible property is a classification rendered as otiose in English law.[241] At present, English law recognizes all types of property as assets, as Worthington instances that property rights can be established over intangible tradeable assets, such as bank accounts being commonly held on trust; the trustee holding a personal right against a bank in trust for its beneficiary.[242]

An additional lacuna may nevertheless lie within the nature of data. What distinguishes data from bank accounts, and cryptocurrency for example is its *non-rivalrous* nature. Simply put, data can be duplicated, and therefore, it is extremely difficult to exclude others. However, as Ben McFarlane posits, "the fact that data does not count as 'property' for one context does not mean that it cannot be 'property' for another, different context."[243] Indeed, Worthington heralds a link to Intellectual Property, stating that despite "the 'property' terminology, the [Intellectual Property] protection delivered by these statutory means is not dependent on any idea of there being 'property' in the creative idea or endeavor."[244] What strategy has the UK legislature taken to resolve this quandary? According to Worthington, intellectual property statutes defines "rights" and thereafter, "remedies" for their infringement.[245] Such rights are then viewed as "assets" which may be the subject of an assignment or any other transfer which the law recognizes, and can be held under a trust.[246] Therefore, although intellectual property rights are non-rivalrous and duplicable, no quandary is created insofar as to its ability to be held under a trust.[247] Given that the non-rivalrous and duplicable dissent does not pose a problem, McFarlane therefore argues that the problem might instead turn to context. According to him, "'[p]roperty' is a very useful

240. Delacroix & Lawrence, *supra* note 9, at 245.

241. *See* Sarah Worthington, *Legal Notions of 'Property' and 'Ownership,' in* Reaching Ownership, Rights and Controls: Reaching a Common Understanding Seminar (Oct. 3, 2018), https://royalsociety.org/~/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf [https://perma.cc/TCG7-Q8VH].

242. *See id*.

243. Ben McFarlane, *Data Trusts and Defining Property*, OXFORD PROPERTY L. BLOG (Oct. 29, 2019), https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property [https://perma.cc/8VHV-BYX7].

244. Worthington, *Legal Notions of 'Property' and 'Ownership,' supra* note 241, at 13.

245. *Id*.

246. *Id*.

247. *Id*.

and powerful concept . . . [and can be] used to help answer a number of different legal questions."[248]

The natural inference from this is that data has not been held as property, limiting the remedies available for damages related to data injuries. For example, Worthington notes that "[i]n most legal systems, information, or 'data', is not an asset."[249] McFarlane views English Trust Law as moving towards a model that is "concerned with situations where equity recognizes that a party (the trustee) holds a right, but is under duties to another (the beneficiary) in relation to that right."[250] Given this formulation, the subject matter of a trust can therefore be conceptualized as a "right against . . . [a] right."[251] The important question stems away from looking towards whether the *nature* of data lends itself well to being established as property under a trust, but instead whether the rights that end-users hold under the GDPR can be held under a trust. As McFarlane ripostes, "to the extent [rights afforded under the GDPR] are correlative of duties owed by data controllers, they should be capable of being held on trust."[252]

The missing step is therefore *assignability* of such rights. It is here where I contend that the data trusts model as unworkable in the current position of English law. This is because to make such rights assignable requires a fundamental re-jig to the current GDPR regime. Presently, the rights to access, portability, and erasure, are not assignable to a third-party. Whether a traditional trusts doctrine will bear fruit then, depends on whether the legislature sees data trusts as a potential way forward, a proposition questionable at present. Supposedly, if the legislature does eventually decide to open the floodgates, then such trusts will become feasible. Inspiration could then be drawn from the current framework undergirding bond trustees, where bondholders pool their funds to a designated company viewed as the custodian of their assets in a way similar to how data trustees could hold data on behalf of their settlors. The property problem can be solved, though uneasily, and with much regulatory intervention.

248. McFarlane, *Data Trusts and Defining Property*, *supra* note 243. *See e.g.*, OBG Ltd v. Allan [2007] UKHL 21, [2008] 1 AC 1 (HL) (appeal taken from Eng.); In re Lehman Bros Int'l (Europe) Ltd (No 4) [2010] EWHC (Ch) 2914 (Eng.).

249. *See* Worthington, *Legal Notions of 'Property' and 'Ownership,' supra* note 241, at 13.

250. McFarlane, *Data Trusts and Defining Property*, *supra* note 243.

251. *Id.*

252. *Id.*

Notwithstanding, English law is moving towards a position favorable to the recognition of digital assets as valid subject matter. In the 2021 case of *Wang v. Darby*, Houseman QC held that "the transfer of digital assets from one account-holder to another . . . could involve or constitute a trust."[253] Indeed, within the context of cryptocurrencies, the 2019 High Court in *AA v. Persons Unknown* has affirmed the definition proposed by the U.K. jurisdiction taskforce.[254] The U.K. jurisdiction taskforce stated that although "[t]he fundamental proprietary relationship is ownership: the owner of a thing is, broadly, entitled to control and enjoy it to the exclusion of anyone else. However, ownership is just one kind of property right: property is a comprehensive term and can be used to describe many different kinds of relationships between a person and a thing."[255] In applying this formulation to the facts at hand, the *AA v. Persons* court held that cryptocurrency assets such as nonfungible tokens might then be held under trust.[256]

If English law continues down this route, a rejoinder of personal information as *property* (as opposed to the rights-based approach) might be another way through the woods. However, this would not be possible unless personal information is present on a form of blockchain system to counteract the duplicability problem, as akin to the blockchain validating Bitcoin or NFT. Therefore, the lack of a blockchain system presents problems in the context of data. For example, Worthington provides the following example: "I own my bicycle. Most people would expect that if it were stolen the law would ensure that I could get back. However, English law holds to the line that even if I can find the thief I am only entitled to money, not to the bicycle."[257] However, it is less clear what would happen in the case of data. Worthington notes that "if you steal information, we both have it."[258] Thus, here Worthington is highlighting the issues associated with data as a form of property. This is exactly the Gordian knot—unlike cryptocurrency under a trust protected by blockchain or a form of unique identifier, blockchain does not form the foundation of ordinary personal data, rendering a property-based

253. [2021] EWHC (Comm) 3054, [89] (Eng.).

254. *See* AA v. Pers. Unknown [2019] EWHC (Comm) 3556 (Eng.).

255. Legal Statement on Cryptocurrency and Smart Contracts, *UK Jurisdiction Taskforce*, p.11 (2019), https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf [https://perma.cc/DT65-MTUU].

256. *See AA* [2019] EWHC (Comm) 3556, [37].

257. Worthington, *Legal Notions of 'Property' and 'Ownership,' supra* note 241, at 11.

258. *Id.* at 13.

rationalization a bark up the wrong tree for the traditional trusts model.[259] Even when considering data collected in the aggregate, such data does "not fall within any statutory definition of protected 'intellectual property.'"[260]

Therefore, charting a reprisal to a rights-based approach might be proper. However, even with legislature intervention to augment rights of portability, erasure, and access as assignable rights, it remains difficult to determine "what *kind of data [should] give[] rise"* to proprietary rights.[261] Three kinds of data might form the spectrum here, as Delacroix and Lawrence argue—data that has been (1) "data that is 'directly provided' by the data subject;" (2) "data such as cookies—for which there is no right to portability;" and (3) "data that is the result of sophisticated processing, such as the data leading to credit rating scores."[262] Though directly provided data heralds property rights favoring the data subject, category two, data such as cookies, opens a can of worms. For data lacking rights to portability, Malgieri argues the resultant property rights should be "exclusionary rights against all commercial actors interested in their data (including the company which has a shared ownership on such data); but the data controllers/businesses will be able to exercise their exclusionary rights against all competing companies but not the data subject."[263] At the end of the sliding scale of kinds of data, category three, data resulting from sophisticated processing, Malgieri views the end-user's property rights as weak, as this data is produced by the "intellectual work of businesses," who "use complex combinations of raw data with specific . . . studies in order to 'create' new data."[264] In such a case, Malgieri argues that such "data [merely] represents 'facts,'" thus users do not require this type of data to be held in a trust.[265]

Taken together, this trifurcation heralds nothing but confusion that arises from a rigid categorization across industry. Though a rights-based approach seems promising, there remains an issue of distinguishing what kinds of rights to grant to differing types of data. Hence, for this approach to take flight in the English law, a fundamental re-jig of current Data

259. *See id*.

260. *See id*.

261. Delacroix & Lawrence, *supra* note 9, at 246.

262. *Id.*

263. Malgieri, *supra* note 189, at 137.

264. *Id.* at 136.

265. *Id.*; *see id.* ("These new data created by companies are not 'real' in the present but allow businesses to predict future behaviour, events, or risks . . . . Therefore, these data can be said to constitute 'trade secrets' in the very traditional meaning of the term.").

Protection Law is required. Although the property right quandary can be resolved, one emerges from the forest with a bag full of confusion.

b. The "Relevance" Quandary

The quandary does not stop simply at the proprietary knot, as shared provenance and scope issues continue to plague the traditional trusts proposal with holes. Here, I bring to light three brambles that chafe uneasily against widespread acceptance of a traditional trust solution in English law.

First, the problem of shared provenance. As Nadezhda Purtova argues, each "piece of data, depending on a particular context, can be personal and non-personal . . . [and thus,] [t]he difficulty lies, first, in determining at which point the level of relation to an individual is sufficient to establish property rights, and second, in tracing the presence of a relation."[266] The latter point, which this Article turns to address, is critical to the analysis as a problem arises from the amorphous form of data in relation to a given person. For example, Delacroix and Lawrence highlight the issue that "many of the 'smart' devices and appliances collecting user data are used in a way that makes it very difficult, if not impossible, to find data that is related to one user only."[267] Thus, there is the related issue of "determin[ing] what is owed to a person leaving a particular data Trust."[268] However, Delacroix and Lawrence note "that current data controllers are already familiar with [such an issue] and each Trust may specify different ways of disentangling data for the purpose of exit procedures."[269]

Importantly, Delacroix and Lawrence do not provide any specific framework to govern the issue. However, the duo does suggest the possibility of an "ecosystem of trusts." In such an ecosystem, for example, one Trust would "specialize[] in direct data management," while another Trust would be "responsib[le] for data management" of the former Trust, allowing the latter Trust to "focus on the policy, rather than the practicalities, underlying data sharing."[270] In the alternative, a different Trust could "work on the basis of a wholly decentralized model, whereby the beneficiaries' data stays wherever it is."[271] Currently, the duo notes

266. Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency*, 10(2) J.L. & ECON. REG. 64, 64 (2017).

267. Delacroix & Lawrence, *supra* note 9, at 251.

268. *Id.*

269. *Id.*

270. *Id.* at 247.

271. *Id.*

that "[a]ny Trust may choose to share data with other Trusts that conform to their constitutional terms."[272] In the context of Trusts that "specialize in only a particular kind of personal data, such as health data . . . [s]uch specialized Trusts are likely to want to negotiate with the more generalist Trusts so as to be able to reap the benefits that come with large-scale datasets."[273]

I, however, respectfully contend that the duo's suggestion does not resolve the problem of data aggregation. Their proposed "ecosystem of trusts" could be feasible in the private market, yet it is uncertain the evolution of data trusts would follow this route when left to the free market. Currently, problems of data provenance and aggregation continue to plague the model of traditional trusts, as end-users are required to identify exactly whether the data held by data trustees relates to them in any way. Further, this proposal depends on industry receptivity of the data trusts model, which though possible, may take years to implement absent regulatory intervention.

Second, the problem of assignability. As a starting point, Article 80(1) states that "[t]he data subject shall have the right to mandate a not-for-profit body . . . to exercise the rights referred to in Articles 77, 78, and 79 on his or her behalf." However, the rights of access, portability, and erasure are not assignable at present. Though Delacroix and Lawrence argue for regulatory intervention, given "the current, well-documented difficulties in exercising the rights to access, portability, and erasure,"[274] the European Commission has yet to initiate any changes. It remains questionable if the Commission will even make such a change, but even so, creating an "ecosystem of trusts" requires a gargantuan effort as mentioned earlier.

Third, the problem of relevance. Chris Reed highlights that "a legal trust must be run for the beneficiaries, [and] not the wider public," limiting the benefits that could be afforded to something like "a charitable trust."[275] Moreover, a legal trust "cannot allow data be used for some socially beneficial purposes if that use does not also benefit the legal trust's beneficiaries."[276] Here, some scholars note that "[t]he 'restrictions of charity law' are referred to without further explanation . . . [but they] assume that the concern was with the rule that property settled on a

272. *Id.*

273. *Id.*

274. *Id.* at 248.

275. Reed, *What is a Data Trust in Legal Terms?*, *in* DATA TRUSTS: LEGAL AND GOVERNANCE CONSIDERATIONS, *supra* note 28, at 12.

276. *Id.*

charitable trust must only be used for charitable purposes."[277] Therefore, "[t]his would exclude 'private' purposes, and would also preclude the trust from having any individually entitled beneficiaries who could enforce the trust."[278]

Does this necessarily pose a problem? I answer not, as the doors of charity law are not implicitly closed to the doctrine of data trusts. Out of the four heads of Charity,[279] scholars propose that "the 'education' head of charity . . . be the most obvious charitable purpose to which a data trusts assets would be devoted."[280] In particular, as "digital files record information and can be analysed," this aligns with the role of the "'education' head of charity [which] includes the carrying out of useful research."[281] Scholars also cite Justice Slade's three requirements from a research trust to be considered a charitable trust: "(a) the subject matter of the proposed research is a useful subject of study; and (b) it is contemplated that knowledge acquired [thereby] will be disseminated to others; and (c) the trust is for the benefit of the public, or a sufficiently important section of the public."[282] Therefore, a data trust imbued with the goal of analyzing information is likely to satisfy Justice Slade's requirements, so long as the research benefitted the public. Following in Delacroix and Lawrence's suggested "ecosystem of trusts," it might thus be contended that certain trusts could be set up as a library of information.[283]

Nevertheless, a dissenter may argue that for data trusts, knowledge dissemination might lead to information tumbling into the hands of users or business entities that seek to use such data for profit-making purposes. Here, scholars note *Incorporated Council of Law Reporting v. AG*, which allowed for a profit-making enterprise to still be considered a charitable trust.[284] The "company [was] incorporated 'for the purpose of recording in a reliably accurate manner the development and application of judge-

277. Jeremiah Lau et al., *The Basics of Private and Public Data Trusts*, 2020 SING. J. LEGAL STUD. 90, 93 (2020).

278. *Id.*

279. *See id.* at 94 ("These [legal requirements of what is considered charitable] are traditionally known as the 'four heads' of charity—the relief of poverty, education, religion, and other purposes beneficial to the public.").

280. *Id.* at 108.

281. *Id.*

282. *Id.* (quoting McGovern v. Att'y-Gen. [1982] Ch 321 (Eng.)).

283. *See id.* at 108-09.

284. *See id.* at 108 (citing Inc. Council of Law Reporting for England and Wales v. Att'y-Gen. [1971] EWCA (Civ) 13 (Eng.)).

made law and of disseminating the knowledge of that law.'"[285] However, the company's profit-making purpose and function did "not detract from the 'primary scholastic function of advancing and disseminating knowledge of the law.'"[286] Analogizing this to data trusts, scholars analogize "a charitable data trust . . . [to] a library."[287] Scholars note that "[a] library can be open to the public, or to particular individuals . . . whose work will further the educational purpose of the charity."[288] In the context of a trust, data could be sent "to a charitable trust or company . . . The trustee or company could then grant access rights to researchers on such terms as the trustees might impose to ensure that their efforts would serve the educational or research purpose."[289] In light of such an example, the contention that a data trust could never function as a charitable trust may be refuted.

c. Tentative Conclusion

My tentative conclusion is that following the traditional trusts approach opens nothing but a can of worms. Although the problems of property and relevance can be solved, as I have shown above, the problems of shared provenance, assignability of rights, and a need to fundamentally re-jig the whole of modern industry practice in an artificial way, renders this approach rather unnatural. In this regard, I propose that fiduciary law provides a way out of the woods in a far more elegant fashion, and in the next subsection, I explore the foundations of UK *ad hoc* fiduciary law, examining whether this lends itself to a tenable solution for English law.

C. An Ad Hoc Fiduciary Approach for English Law?

The seminal case concerning the doctrinal nature of fiduciary relationships in English law is *Bristol v. Mothew*, where a fiduciary is described as "someone who has undertaken to act for or on behalf of another in a particular matter in circumstances which give rise to a relationship of trust and confidence."[290] Included within a duty

285. *Id.* (quoting *Inc. Council of Law* [1971] EWCA (Civ) 13, [103]).
286. *Id.*
287. *Id.*
288. *Id.* at 108-09.
289. *Id.* at 109.
290. Michael Green et al., Fiduciary Duties in International Litigation and Arbitration (Chancery Bar Association Shanghai Conference, 2018), https://www.chba.org.uk/for-members/library/overseas-seminars/fiduciary-duties-in-international-litigation-and-arbitration

undertaken by a fiduciary, "[the] fiduciary must act in good faith . . . must not make a profit out of his trust . . . [nor] place himself in a position where his duty and his interest may conflict."[291] Thus, this suggests that the *core trait in English law* of a fiduciary is that of loyalty. For this Article's argument to take flight, one must examine how the runway has been laid by the English Courts.

To date, two key blocks of *ad hoc* fiduciary relationships decisions have emerged across English jurisprudence, albeit on thin ice. The first block finds itself in the vendor-purchaser context. In *English v. Dedham Vale Properties Ltd*, the court held that the "the categories of fiduciary relationships which give rise to constructive trusteeship should be regarded as falling into a limited number of strait-jackets or as being necessarily closed."[292] Rather, the test was whether "the relationship in the eyes of equity a fiduciary one in the sense that it imposed relevant fiduciary duties on the defendant towards the plaintiffs."[293] Ultimately, the court viewed the permutation of facts as sufficient to engender an *ad hoc* fiduciary relationship because the planning permission "if disclosed to the vendor, might reasonably be supposed to be likely to influence him in deciding whether or not to conclude the contract."[294] Therefore, although a purchaser-vendor relationship did not fall into the usual status-based categories, a fiduciary relationship arose.

The second block finds itself in the joint-venture context. Here, scholars note that in *Ross River Ltd v. Waverly Commercial Ltd*, the court "identified three important cases which have considered the nature of the fiduciary obligations that can arise in the context of joint ventures."[295] It is argued that examining *why* the English court found an *ad hoc* fiduciary relationship on the facts will likely enable us to extract general principles to assist in supporting an *ad hoc* fiduciary duty in the online service providers context.

In *Murad & Murad v. Al-Saraj & Westwood Business Inc*, the court determined that a business riposte to acquire a hotel was sufficient to augment a fiduciary relationship, because "the defendant had taken on a

[https://perma.cc/TQ34-UB45] (quoting Bristol & W. Bldg. Soc'y v. Mothew [1996] EWCA (Civ) 533, [1998] Ch1, 18 (appeal taken from Eng.).

291. *Id.* at 1-2.

292. [1978] 1 WLR 93 (Ch) at 110 (Eng.).

293. *Id.*

294. *Id.* at 111.

295. Green et al., *supra* note 290, at 4 (citing Ross River Ltd v. Waverly Com. Ltd [2012] EWHC 3006 (Ch) (Eng.)); see also Murad & Murad v. Al-Saraj & Westwood Bus. Inc. [2004] EWHC (Ch) 1235 (Eng.); JD Wetherspoon Plc v. Van De Berg & Co [2009] EWHC (Ch) 639 (Eng.); John v. James [1991] FSR (Ch) 397 (Eng.).

number of responsibilities in connection with the joint venture, in some respects acting as the claimants' agent."[296] This imbalance was further exacerbated by the claimants' lack of "relevant experience, [as] they had no knowledge of the arrangements made by defendant with third parties and they trusted the defendant with extensive discretion to act in relation to [the joint] venture."[297] In *JD Wetherspoon Plc v. Van De Berg & Co*, the court determined "a special relationship of trust and confidence" existed by virtue of the relationship of chairman to director.[298] However, this case was particularly apt in highlighting the fact-sensitivity of fiduciary relationships, as two other directors were determined to not owe such a duty.[299] In *John v. James*, "the claimant, Elton John, asserted fiduciary duties against his manager, publisher and associated companies under agreements for the exploitation of compositions, accompanied by the assignment of the copyright in the compositions."[300] Notably, here "[t]he defendant was found to owe fiduciary duties to John even though the copyrights were assigned outright to the defendant and the defendant had its own interest in exploitation of the compositions."[301]

What might the above trilogy teach us? Scholars summarize "general points [that] can fairly be said to emerge from these authorities."[302] First, I agree that from these three cases, the current state of UK *ad hoc* fiduciary law can be summarized into three principles. First, *Ross* River and *John v. James* point out that "[c]ontrol of relevant matters, such as negotiation or ownership of assets, is a particularly strong indicator of the reliance likely to have been placed on one party by the other."[303] Here, the English courts seem to veer towards a finding of an *ad hoc* fiduciary relationship should it be *more likely* that the present relationship seems akin to a traditional *status-based* one. Second, "[t]he nature of the fiduciary obligations owed is itself a fact-sensitive enquiry to be determined by the nature of the relationships before the court."[304] Thus, "[i]n an appropriate context, the duties owed will extend beyond a fiduciary duty of good faith."[305] Third, *Murad & Murad* and *JD Wetherspoon* support the proposition that when "assessing the nature of

296. *Id.*
297. *Id.*
298. *Id.*
299. *See id.*
300. *Id.* at 4-5.
301. *Id.* at 5.
302. *Id.*
303. *Id.*
304. *Id.*
305. *Id.*

the obligations assumed or owed by the parties, the court may well look through the structures established for the purpose of carrying out a joint venture, or . . . to the underlying relationship between the claimant and defendant."[306]

Taken together, a general proposition might indeed be formulated for *ad hoc* fiduciaries in English law, which I believe likely consists of five key factors. In most English cases, courts are likely to examine the (i) vulnerability of one party vis-à-vis another in the course of their relationship; (ii) whether the facts at hand are analogous to one of the "classic *status-based*" fiduciary relationships already recognized under English law; (iii) how reasonable it was for a claimant to expect that a defendant would protect his own interest (taking into account various factors such as control of relevant matters, and ownership of assets); (iv) whether the parties held any unspoken mutual expectations, and a general weighing up of the (v) fairness of outcome when determining whether an *ad hoc* fiduciary relationship arise. Hitherto, this paper is now pre-disposed to apply this analytical framework to the online service provider context and examine its merits vis-à-vis the traditional trusts approach.

D. Applying an Ad Hoc Fiduciary Framework for Online Service Providers in English Law

Part II.a.iv canvassed an extensive analysis of how an online service provider may engender a relationship of vulnerability due to the vast difference of expertise vis-à-vis the consumer. Looking to my first identified factor, vulnerability of one party vis-à-vis another in the course of their relationship, I believe that this is likely satisfied in most cases involving online service providers and end-users.

Recent developments in the United Kingdom augments such a proposition. There, a £2.3 billion class-action lawsuit was recently brought against Facebook's UK arm in January 2022.[307] The class action representative Liza Gornsen, Senior Advisor to Britain's Financial Conduct Authority, alleged that Facebook "made billions of pounds by imposing unfair terms and conditions that demanded consumers surrender valuable personal data to access the network."[308] According to Liza

306. *Id.*

307. Kirstin Ridley, *Facebook Faces $3.2 bln UK Class Action over Market Dominance*, REUTERS: TECH. (Jan. 14, 2022, 12:10 AM), https://www.reuters.com/technology/facebook-faces-32-bln-uk-class-action-over-market-dominance-2022-01-14/ [https://perma.cc/8PYP-BBGA].

308. *Id.*

Lovdal Gornsen, "[i]n the 17 years since it was created, Facebook became the sole social network in the UK."[309] Thus, Facebook clearly had achieved a monopolistic dominance in the market. Moreover, Facebook "abused its market dominance to impose unfair terms and conditions on ordinary Britons, giving it the power to exploit their personal data."[310]

Similarly, in *Vidal-Hall v. Google Inc.*, the English Court of Appeals imposed statutory sanctions via Section 13(2) of the Data Protection Act 1998 because Google had collected information about its users' browsing habits via cookies placed on their devices without their consent and in breach of Google's privacy policy.[311] Taken together, it is evident that a situation of vulnerability is engendered; and in most cases going before a court involving a relatively large online service provider, (i) will be fulfilled.

As to my second identified factor, whether the facts at hand are analogous to one of the "classic *status-based*" fiduciary relationships already recognized under English law, a tenable argument may be made that online service providers, are akin to the situation found in *English v. Dedham*. This is because said service providers are expected to handle the user's data with care, disclosing the necessary boundaries of *how* each end-user's data will be used and prevent themselves from straying any limits. While handling a user's personal data, one might analogize the online service provider as a "self-appointed agent," for an online service provider is thought to handle an end-user's data on the user's behalf, to improve their online experience to permissible limits.

My third identified factor, how reasonable it was for a claimant to expect that a defendant would protect his own interest, online service providers may reasonably assert a need to protect end-user's interests. As Ian Kerr notes, "the current architectures of the networked world allow providers access to their users' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or arms of government."[312] Thus, "an online service provider acting *mala fides* . . . could convert a user's [personal information] to its own or to another's advantage, disclose confidential information to a competitor, turn over otherwise privileged evidence in the course of criminal or private litigation, and so on."[313] Dissenters may

309. *Id.*

310. *Id.*

311. *See* [2014] EWHC (QB) 13.

312. Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35(3) CAN. BUS. L.J. 419, 454 (2001).

313. *Id.*

nevertheless adopt the same argument line of Khan and Pozen, asserting that it would also be reasonable for online service providers to act according to its shareholder's interest. However, a plausible rejoinder finds itself in Section 172 of the English Companies Act, which is the UK's equivalent of the Delaware Business Judgment Rule.[314]

Section 172(1) states that "[a] director of a company must act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole." Yet, a Gordian knot arises as "success of the company" remains undefined, though in the absence of any other indication in the company's constitution, the success of a company is defined as its long-term financial success.[315] Various scholars have attempted to interpret the meaning of this term, eventually coming to a consensus of where the common law lies. David Kershaw, for example, has highlighted the "board must not only have regard to the interests of the current value of the company's shares but also the long-term value of the company."[316] On the other hand, Paul Davies states the "better view" as being that directors "[have to] consider both the long . . . and the short-term interests of the shareholders and strike a balance between them."[317]

I argue, however, that an escape rope nevertheless exists. Directors, in the absence of specific instruction from shareholders, whilst acting in good faith, possesses a level of latitude when deciding on the definition of "success."[318] Here, many scholars have termed Section 172's duty as one of "enlightened shareholder value."[319] This idea is supported by directors being mandated to consider "the likely consequences of any decision in the long term,"[320] the impact of "the company's operations on the community and the environment,"[321] and finally, the desirability of the "company maintaining a reputation for high standards of business

314. *See* Companies Act 2006, c. 46, § 172(1) (UK).

315. *See* Companies Act 2006, c. 46, § 172(2) ("Where or to the extent that the purposes of the company consist of or include purposes ither than the benefit of its members, subsection (1) has effect as if the reference to promoting the success of the company for the benefit of its members were to achieving those purposes.").

316. DAVID KERSHAW, COMPANY LAW IN CONTEXT 337 (2d ed. 2012).

317. PAUL L. DAVIES ET AL., PRINCIPLES OF MODERN COMPANY LAW 10-035 (11th ed. 2021).

318. See, e.g., Explanatory Notes, s172, [327], Companies Act 2006, c.46 (UK) ("The decision as to what will promote the success of the company, and what constitutes such success, is one for the director's good faith judgment.")

319. DAVIES ET AL., *supra* note 318, at 10-027.

320. Companies Act 2006, c. 46, § 172(1)(a).

321. *Id.* § 172(1)(d).

conduct."[322] Though "[t]his list is not exhaustive, [it nonetheless] highlights areas of particular importance which reflect wider expectations of responsible business behaviour."[323]

How might this be applied onto online service providers? As discussed in Part II.a.iv, when applying the Delaware Business Judgment Rule, the duty of loyalty to shareholders is not inherently conflicted with the duty of loyalty to end-users regarding their personal data. Likewise, ensuring compliance with data protection best practices is also desirable to maintain "high standards of business conduct."[324] ESG considerations have taken center stage in recent times and will likely adopt an upward trend going forward.[325] Such considerations are certainly even more relevant as shareholders become more convinced of the benefits of ESG investing.

As to my fourth identified factor, whether the parties held any unspoken mutual expectations, there is industry data to suggest the existence of implied mutual understandings in the online service providers context. In 2015, the UK Competition & Market Authority conducted research on Commercial Use of Data to further understand the expectations UK end-users hold vis-à-vis their personal data, highlighting data obtained from various studies.[326] For example, the report noted a study "found that almost all consumers (98%) thought some personal data and information was collected by 'free-to-use' online services and social media."[327] Here, 70% of online and social media end-users stated that they had "wide ranging expectations of what data companies gather," often commonly on the ambit of "search history, sites visited, 'likes,' locations and purchases."[328] However, only 22% of end-users actually understood what information was exactly being collected.[329] Thus, the above statistics appear to show a dissonance between *form* and *substance*: end-users understood online service providers were collecting data, but the end-

322. *Id.* § 172(1)(e).

323. Explanatory Notes, s172, [326], Companies Act 2006, c.46 (UK).

324. Companies Act 2006, c. 46, § 172(e).

325. *See* Sharon E. Smith, *UK Company Law Change Could Make Section 172 Fit for Purpose*, PINSENT MASONS (Apr. 20, 2021, 2:31PM), https://www.pinsentmasons.com/out-law/analysis/uk-company-law-change-could-make-section-172-fit-for-purpose [https://perma.cc/6A86-5XM9].

326. *See The Commercial Use of Consumer Data*, CMA (June 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf [https://perma.cc/N7XR-9FU7].

327. *Id.* ¶ 4.8, at 98.

328. *Id.* ¶ 4.12, at 99.

329. *Id.* ¶ 4.13, at 99.

users simply did not know *how* exactly their data was used by companies. This dissonance was echoed by survey respondents who indicated that they felt a loss of control over the privacy of their data once it has been handed over to an online service provider.[330]

Research has shown the current uncertainty is largely due to online service providers not having made such implied mutual understandings *express*. Some reports found that 42% of end-users felt uninformed about "the conditions and uses of their personal information," while other reports determined "59% of the [mobile] apps [surveyed] 'left users struggling to find basic privacy information.'"[331] Further, end-users have expectations related to the perceived value of their personal data. One report found that "62% [of consumers] agreed that they should be paid a fee by organisations using their data."[332] Thus, online service providers, while blatantly aware of the mutual implied understandings with end-users, are likely to have taken advantage of this inaction in asserting their dominance vis-à-vis the end-user's personal data.

Lastly, my fifth identified factor, fairness of outcome when determining whether an *ad hoc* fiduciary relationship arise, remains uncontentious, considering all that has been discussed. The current information asymmetry and the abuse of a dominant position by online service providers renders a fiduciary relationship particularly apt and fair in the given context.

In the final analysis, I argued that an *ad hoc* fiduciary rationalization between online service providers and end-users can arise with the objective of imbuing the end-user with a *bottom-up* workable enforcement mechanism that possesses some teeth in English law. This caused me to diverge from the traditional trusts model proposed by Delacroix and Lawrence, given the problem of shared provenance issues, assignability of rights, and the need to fundamentally re-jig modern industry practices in an artificial way. Prior to moving to the final part of this Article, I it is worth exploring the current scholarly dissent against the stability of an *ad hoc* model. In the next subsection, I seek to strike down such contentions, ultimately concluding that an *ad hoc* rationalization is workable to act as the bastion which guards the online service provider and end-user relationship.

330. *Id.* ¶ 4.66, at 116.
331. *Id.* ¶ 4.32, at 104-05.
332. *Id.* ¶ 4.29, at 103.

E. Shaking the Substratum of the Fiduciary Doctrine

Despite the earlier subsections having set out the black-letter law, English Fiduciary Doctrine continues to remain in flux, particularly amidst the clash between English scholars on the exact formulation of *what* the substratum of the fiduciary doctrine ought to be tending towards. James Edelman, for example, has argued a shift of focus towards a debate from that of identifying "which relationships are fiduciary, based on notions of status or relationship, to a focus upon whether duties are expressed or implied in relationships involving manifestations of voluntary undertakings."[333] According to Edelman, "[f]iduciary duties arise in the same manner as any other express or implied term: by construction of the scope of voluntary undertakings."[334] Put simply, Edelman contends that fiduciary duties ought to be centered on the concept of consent, arguing that instead be undergirded by an idea of consent, being at pains to argue that "a voluntary undertaking . . . is a necessary condition for any fiduciary duty."[335] To him, this is largely akin to the test for the implication of terms, particularly when a relationship is not outrightly stated from the get-go.[336]

Paul Miller, however, locks Edelman by the horns and corners him into submission. Miller asserts Edelman's approach as offering "little explanatory yield," citing three main reasons as bases for this assertion.[337] First, Miller notes that fiduciary relationships are "sometimes . . . established constructively, and consent is never in itself sufficient to make a relationship fiduciary."[338] Second, Miller criticizes Edelman's proposed factors in identifying a fiduciary relationship. Miller argues that Edelman relies on the premise that "[f]iduciary relationships generate fiduciary duties," and therefore, fails to address "*why* fiduciary relationships generate fiduciary duties."[339] Third, Miller notes that Edelman does not explain "why the law insists upon [a voluntary] undertaking as a condition of entering a fiduciary relationship."[340] Ultimately, Miller criticizes Edelman's doctrinal model as "reductivist and instrumentalist."[341]

333. James Edelman, *When Do Fiduciary Duties Arise?*, 126 L.Q.R. 302, 325 (2010).
334. *Id*. at 302.
335. *Id.*
336. *Id*. at 308.
337. Paul Miller, *Justifying Fiduciary Duties*, 58(4) MCGILL L.J. 969, 986-87 (2012).
338. *Id*. at 986.
339. *Id*. at 987.
340. *Id.*
341. *Id*. at 1004.

As an alternative, Miller proposes a "juridical justification," noting "that fiduciary duties are distinctive and supported by reasons derived from formal properties of the fiduciary relationship."[342] These distinctions stem in part from "one person (the fiduciary) exercis[ing] discretionary power over the practical interests of another (the beneficiary)."[343] Therefore, Miller posits that "[f]iduciary power is a form of authority derived from the legal capacity of the beneficiary or a benefactor."[344] Lastly, Miller asserts that "[t]he normative status of fiduciary power is that of a means belonging exclusively to the beneficiary."[345] In this regard, Miller takes a more *inward* approach into examining the justification for a fiduciary relationship, as opposed to Edelman who extends an excessive focus on *voluntariness* to shepherd the doctrine towards contract law.

What might this mean for the *fact-based* fiduciary relationship rationalization proposed in this Article? Although Edelman's theory might pose a necessary Gordian knot as "fiduciary obligations . . . in the commercial context . . . always require a preexisting relationship with a voluntary undertaking by the fiduciary," this is not the law as accepted at present.[346] Miller rightly points out that such an analogy with "implied terms of contract" is inapt.[347] I believe that Miller's view reaffirms the rationalization set out in this Article at Part III.C, particularly when considering his trifurcated analysis. Miller notes that among other factors, "inequality, dependence, and vulnerability" undergirds the substratum of a fiduciary relationship.[348] Moreover, these factors have been shown to be especially present as online service providers increasingly gain a strong foothold over the end-users of today.

Continuing the examination of this issue, it is also apposite to examine the bell that Sarah Worthington has sounded for English law. According to Worthington, defining who is a fiduciary in part "because rather dramatic obligational and remedial advantages come with the fiduciary law," while Worthington also notes that "[i]n England we have not troubled ourselves much by these boundaries."[349] Thus, Worthington suggests that English law may be a tenable way to approach the issue of defining a fiduciary. Worthington first analyzes the differences between

342. *Id.* at 1023.
343. *Id.*
344. *Id.*
345. *Id.*
346. Edelman, *supra* note 333, at 310.
347. Miller, *Justifying Fiduciary Duties*, *supra* note 337, at 981.
348. *Id.* at 1011.
349. Sarah Worthington, *Four Questions on Fiduciaries*, 2(2) CJCCL 723, 729 (2016).

a solicitor and plumber, noting that we "invest both with discretions to exercise on [one's] account, and [are] compelled to trust both with decisions which affect [our] welfare and [our] finances."[350] The difference between a plumber and a solicitor, however, is called into focus when examining when such individuals cross the line of trust. In the context of loyalty, Worthington observes that "[t]he line is not crossed simply because we have handed over some part of our autonomy to another, or . . . invested another with powers and discretions which must be exerted in the interests of the principal and not the fiduciary power-holder."[351] Importantly, the factor at the heart of the fiduciary relationship, regardless of whether the fiduciary is a "power-holder," "is that the purpose of the exercise of the powers is unequivocally to advance the principal's interests, and any considerations which call into play the fiduciary's interests are either 'irrelevant considerations' or reflect 'improper purposes.'"[352]

Worthington cites the UK Law Commission's finding related to the tests of whether a fiduciary relationship is established,[353] but argues that "the real question is whether the law will insist that this expectation [of a fiduciary duty] . . . is delivered."[354] To answer that question, Worthington "suggest[s] that our language is impeding our analysis."[355] Here, Worthington notes that the law often defines people based on obligations to others, yet Worthington argues that the "functional" nature of the relationships should push us "from the language of people-labelling to the language of obligation-labelling."[356] Worthington also notes the peculiarity that fiduciaries "are required to put the other's interests *ahead* of their own, and to the extent that they do not do this they will have to disgorge the benefits thereby obtained."[357] Though beginning to question "when are obligations of self-denial *needed*," ultimately Worthington avoids answering that question to push her proposal deeper into the rabbit hole.[358] Worthington notes that "[a] move on language is unlikely to be the only moved needed in delivering a tighter analysis of 'who is a

350. *Id.* at 728.

351. *Id.* at 730.

352. *Id.*

353. *See generally* LAW COMMISSION, FIDUCIARY DUTIES OF INVESTMENT INTERMEDIARIES, Law Com No. 350 (July 1, 2014).

354. Worthington, *Four Questions on Fiduciaries*, *supra* note 349, at 731.

355. *Id.* at 733.

356. *Id.*

357. *Id.* at 734.

358. *Id.*

fiduciary.'"[359] For example, Worthington points out that the "fiduciary no-conflicts rule is, at base, directed at ensuring that the fiduciary does not *compete* . . . [but] [i]t says nothing about carrying out the tasks which are assigned."[360] Here, Worthington describes the difference between a company director and a solicitor, with the former as a prime example of an "when . . . a 'non-compete' rule essential."[361] Ultimately, rather than explicitly defining who is a fiduciary, Worthington asserts "a claim for more (or even more) rigorous analysis of the fiduciary terrain and careful exposure of its detail."[362]

Worthington's analysis proves an interesting repartee, although her article merely prompts a leap out of the frying pan and into the fire. However, her analysis does not drive a shaft into the *fact-based* rationalization proposed in this Article, particularly when considering her analysis on solicitors and other similar individuals. Unlike solicitors, end-users are often inadequately protected by the existing duties proscribed to online service providers and lack sufficient remedies for breaches of trust. Though Worthington's examination of English fiduciary law's corpus is helpful, she stops short of asserting a firm conclusion. Thus, there is room for this Article's assertion of characterizing online service providers through a *fact-based* fiduciary rationalization. Notably, the fact-based analysis conceptualizes fiduciary relationships as forming from certain *characteristics* that undergird the fiduciary and end-user, and hence prevents a *prima facie* determination of such relationships. An obligations focused analysis is, therefore, one appropriate way forward, and imposes a no-conflict duty, which is especially relevant for online-service providers.

Taken together, I have shown that the academic views detracting from the present state of case-law is a bark up the wrong tree. Of course, the present state of English law is not satisfactory as well, particularly for *fact-based* fiduciaries, and a more radical re-jig is needed in the long run. Therefore, a *fact-based* rationalization for English law is sufficient to augment the relationship between online service providers and end-users with sufficient ammunition to guard against the risk of data misuse. This is an effective *bottom-up* mechanism that will resolve the quandary that the GDPR framework currently lacks in English law.

359. *Id.* at 735.
360. *Id.*
361. *Id.*
362. *Id.* at 764.

IV. COMPLEMENTING EXISTING TOP-DOWN REGIMES TO ENFORCE EFFECTIVE DATA PROTECTION

Having made the argument that a *fact-based* fiduciary approach is most preferable going forward for both U.S. and UK law, the final voyage this Article must chart towards before finding anchor asks whether these models sit well with existing sectorial-based data protection regulations in the U.S. and the general framework of the UK-GDPR in the UK. Quick comments will be made on each limb, with each step further unravelling the Gordian knot once introduced in the start.

A. English Law

Paul Schwartz and Karl-Nikolaus Peifer posit that the two jurisdictions have largely bifurcated in terms of their approach to *top-down* regulation: the European Union (EU) and the United States.[363] "In the EU, data protection is a fundamental right anchored in interests of dignity, personality, and self-determination."[364] Indeed, although Brexit has freed the UK from the fetters of EU law, and thereby from being subservient to the GDPR, an almost identical provision to the GDPR has been retained in domestic law (UK GDPR), with the "key principles, rights, and obligations remain[ing] the same."[365] Thus, given that no existing legislative developments have been tabled by the English Parliament at present to modify the existing regime, it is worth examining the core rationale of the GDPR and why it was enacted.

Schwartz and Peifer identify the nub of privacy in the EU, which stems from the European Convention of Human Rights. There, Article 8 imbues "the individual 'a right to respect for his private and family life,'" thus forming the cornerstone of privacy in European Law jurisprudence.[366] The Charter of Fundamental Rights brings the idea of privacy a step further, with Article 8(1) providing that "[e]veryone has the right to the protection of personal data."[367] The principles emaciated in

363. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Laws*, 106 GEO. L.J. 115 (2017).

364. *Id*. at 123.

365. *The UK GDPR*, ICO, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/ (last visited Mar. 13, 2023) [https://perma.cc/PG7E-JMWX].

366. Schwartz & Peifer, *supra* note 363, at 125 (quoting Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222). Charter of Fundamental Rights of the European Union, art. 8(1), 2000 O.J C 364/10)).

367. *Id*. (quoting Charter of Fundamental Rights of the European Union, art. 8(1), 2000 O.J C 364/10)).

the Charter have been holistically reflected throughout the various judicial actors in the European Law community—the European Court of Justice, the European Court of Human Rights, and other conversations with fellow Member States.[368] More importantly, the EU's approach may be distinguished from that of the United States by its extension of rights to private-private party relations. Schwatz and Peifer note this has been accelerated by the "horizontal effect" of EU law, extending constitutional rights to privacy and data protection to private-private relations.[369] Thus, as Schwatz and Peifer aptly note, "[t]he resulting European data protection systems centers itself around the data subject as a bearer of rights."[370]

Yet, the flames of this torch bearer are nevertheless fettered—at present, enforcement mechanisms seem limited to class action lawsuits. Article 82 of the GDPR reads "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[371] Some scholars note, however, the right to compensation "seems illusory."[372] Theory and practice appears to diverge because an "overall overview of cases from the national courts" have yet to bear fruit.[373]

Amidst the scarce case law, three jurisdictions in the EU are of particular interest—Austria, Netherlands, and Germany. In Austria, the claimant argued before the Austrian Oberlandesgericht (OLG) that the defendant had offended his data protection rights by publishing the claimant's political opinions.[374] Here, the primary dispute focused on whether a breach of the GDPR by a data controller ought to trigger an automatic right to a claim for damages under Article 82(1) of the GDPR. Ultimately, the OLG concluded that a certain threshold of "non-material

368. *See also* Joanne Vengadesan & Nora Pook, *United with Differences: Key GDPR Derogations Across Europe*, PENNINGTONS MANCHES COOPER (Mar. 26, 2019), http://penningtonslaw.com/news-publications/latest-news/2019/united-with-differences-key-gdpr-derogations-across-europe [https://perma.cc/RH27-E2UL].

369. *See* Schwartz & Peifer, *supra* note 363, at 126.

370. *Id.*

371. GDPR, *supra* note 229, art. 82.

372. Mona Naomi Lintvedt, *Putting a Price on Data Protection Infringement*, 12(1) INT'L DATA PRIVACY L. 1, 13 (2022).

373. *Id.* at 12.

374. Oberlandesgericht [OLG] Innsbruck, Feb. 13, 2020, 1R182/19b, https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20200213_OLG0819_00100R00182_19B0000_000/JJT_20200213_OLG0819_00100R00182_19B0000_000.pdf (Austria).

damage" was necessary to demonstrate sufficient harm.[375] By contrast, the Supreme Court of Amsterdam presented a more substantive argument that Article 82(1) does provide independent enforcement rights.[376] There, the court concluded that the "mere violation of fundamental rights does not automatically result in damages."[377] Similarly, German courts have favored a stricter construction of Article 82.[378]

Ultimately, scholars have concluded that EU Jurisprudence has set "low damages or high thresholds for casualty . . . [and] [t]he requirement for proving damage is considerably higher than the threshold which the DPAs [Data Protection Authorities] apply when issuing administrative fines."[379] Even if compensation is awarded, cases have shown that the remedy may be merely symbolic. Thus, the procedural costs invoked would likely exceed the expected remedy (if even awarded) in most cases and bringing a case on one's own account is a herculean effort.

In the context of English law, the UK Supreme Court has recently considered the issue of what damage meant in the appeal of *Lloyd v. Google LLC*.[380] There, the parties struggled to construe "damage" in the context of Section 13(1) of the Data Protection Act of 1998, wherein the Supreme Court referred to EU law as a guide.[381] Here, the court maintained a strict construction as to the interpretation of damage, akin to the definition offered in *Vidal-Hall*.[382] Although both EU and English law recognize privacy as an important constitutional right, the mechanism for *bottom-up* enforcement is at present simply confused. Even if there appears to be a viable mechanism for individual enforcement, EU jurisprudence has shown that an Article 82 challenge is only brought by very few litigants because of the low success rate and high litigation costs. Imposing a *bottom-up* mechanism with some teeth through the proposed *fact-based* fiduciary rationalization therefore complements the *top-down*

375. *Id.*

376. Uitspraak 201905087/1/A2 (Apr. 1, 2020), https://www.raadvanstate.nl/@120629/201905087-1-a2/ (Amsterdam).

377. *See id.*

378. *See e.g.*, Dresden Oberlandesgericht [Dresden OLG] [Higher Regional Court] June 11, 2019, 4 U 760/19 (Ger.); *Amtsgericht Diez Schlussurteil v.07.11.2018* – 8 C 130/18 (2018), https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20Diez&Datum=07.11.2018&Aktenzeichen=8%20C%20130%2F18.

379. Lintvedt, *supra* note 373, at 13.

380. *See* Lloyd v. Google LLC [2021] UKSC 50 (UK).

381. *See id.* at [119]-[123].

382. *See id.*; *see also* Cynthia O'Donoghue & Sarah O'Brien, *Lloyd v. Google: Supreme Court Rejects Compensation Claim*, REED SMITH: TECH. L. DISPATCH (Nov. 22, 2021), https://www.technologylawdispatch.com/2021/11/in-the-courts/lloyd-v-google-supreme-court-rejects-compensation-claim/ [https://perma.cc/G7ZP-N572].

framework of the UK-GDPR well, because a well-managed *fact-based* fiduciary rationalization clears up the confusion regarding Article 82(1) of the UK-GDPR, enabling litigants to seek salvation of their privacy rights through the common law instead of a questionable EU law-inspired Article. This furthermore enables complementary enforcement with the vigorous *top-down* mechanism which is already available *viz*. the UK-GDPR. Therefore, this Article argues the *fact-based* rationalization proposed must be the way forward for English law.

B. U.S. Law

In juxtaposition to the EU, Schwartz and Peifer view most U.S. statutes as placing "the individual squarely in marketplace relations, whether as a consumer, customer, or 'subscriber' of telecommunications."[383] More notably, the duo posits that "U.S. law does not equip the privacy consumer with fundamental constitutional rights; rather, she participates in a series of free exchanges involving her personal information."[384] In the United States, "[t]here is no constitutional right to information privacy" in the private sector, and "[i]n the public sector, there is only a limited interest in information privacy," namely the Fourth Amendment and the Due Process Clause of the Fourteenth Amendment.[385] As Schwartz and Peifer note, "[a]t best, the Fourth Amendment provides a judicially-enforced warrant requirement against a limited group of law enforcement activities."[386] Similarly, "constitutional scrutiny [under the Fourteenth Amendment] by federal courts tends to be undemanding."[387] Thus, there is clear, striking difference when comparing the EU to the United States as the latter "lacks any analogous right to data protection and informational self-determination."[388]

The lack of an overarching data protection law, further exacerbated by the weak constitutional recognition of privacy as a fundamental right, leads to an uneasy Gordian knot binding the protection of end-users in the U.S. online arena. As Schwatz and Peifer note that "U.S. law does not protect the individual through an omnibus law. Rather, information privacy law takes the form of a patchwork that includes statutes as well as regulations at both the federal and state level."[389] Indeed, the U.S. only

383. Schwartz & Peifer, *supra* note 363, at 132.
384. *Id.*
385. *Id.* at 132-33.
386. *Id.* at 133.
387. *Id.* at 134.
388. *Id.*
389. *Id.* at 136.

seeks to intervene in the most extreme of cases, which is why Delacroix and Lawrence have viewed a *top-down* approach as lacking any teeth.

The bleak vision of data protection in the United States explains why a *fact-based* fiduciary theory proposed in this Article is apposite. Scattered statutory law prevents end-users from identifying their rights, leaving such users thrown unknowingly into the wilderness of the data ecosystem. Developing a *bottom-up* approach fits well with the search for a middle-ground to protect data in the United States. This will allow a healthier ecosystem to emerge, therefore resolving the end-user quandary which policy makers have been faced with thus far.

V. CONCLUSION

This Article started off with a goal to evaluate whether current *top-down* regulatory approaches and a proposed data trust solution served to be merely a fig leaf or a proper bastion to unravel the Gordian knot surrounding online service providers. Part I showed the answer as the former, because such strategies lacked little substantive teeth, ambitious as they might be. Thereafter, this Article charted a different course in Part II, steering through the seas of fiduciary law. There, this Article utilized Balkin's seminal fiduciary thesis as a starting point, though it ultimately diverged from Balkin's rationalization by developing an independent *fact-based* fiduciary theory to bind online service providers to task via the end-user. The reason the *fact-based* fiduciary theory is preferable is because existing U.S. case law concerning *fact-based* fiduciaries is sufficiently robust to engender an adequate analogy with online service providers. This argument is further augmented by addressing Khan and Pozen's dissent against a fiduciary rationalization, especially after showing that the quandary relating to conflict of interests can be resolved. Ultimately, an *ad hoc* fiduciary rationalization appears to be the best approach to hold online service providers to account in U.S. law.

Part III then journeyed to the world of traditional data trusts, yet weaknesses in this approach were soon evident. This Article explored if a fact-based fiduciary rationalization was plausible in the context of English law, given said weaknesses in the traditional data trusts approach. Here, I concluded that the fact-based doctrine holds slightly weaker foothold as compared to U.S. law—because of the relatively undeveloped nature of fact-based fiduciary relationship principles in English law. However, by distinguishing Edelman and Worthington's contentions, this Article was able to draw a tenable conclusion that the fact-based approach is indeed the most stable way forward. Part IV finally examined current *top-down*

regulatory frameworks in detail, and the different normative bases found in the United States versus the EU. However, both jurisdictions prevent an end-user from possessing a clear framework to enforce their rights. This Article then argued the *fact-based* fiduciary rationalization as equipping with the *end-user* with a *bottom-up* approach that holds sufficient teeth to undergird a stable repartee against online service providers.

In George Orwell's novel, *1984*, the protagonist Winston Smith realized "for the first time that, [if] you want to keep a secret, you must also hide it from yourself."[390] In a world where one lacks understanding of his autonomous personal data rights, further exacerbated by the lack of a *bottom-up* attack in the hands of end-users, online service providers are likely to continue taking the reins of end-user's personal data and herald the continued trend of systemic data abuse. Here, the *fact-based* fiduciary rationalization, as proposed earlier, will enable end-users to finally take the reins in starting a constructive debate with online service providers. An effective deterrent is needed to prevent further misuse of data, and as argued, the *fact-based* rationalization is sufficient to escape this rabbit hole. If successful, this will finally pressure online service providers to hit a threshold of higher prudency when managing an end-user's data.

Shakespeare, in *Henry V*, Act 1 Scene 1, 45-47 posited:

Turn him to any cause of policy,
The Gordian Knot of it he will unloose,
Familiar as his garter.[391]

As what unfolded in the legend of Phrygian Gordium, Alexander the Great solved an intractable problem easily by finding a solution that renders the perceived constrains of the problem null and void. This Article does not promise that the proposed *fact-based* rationalization will unravel the Gordian knot of data misuse instantly, but it is with hope that history may repeat itself in the coming future. As argued in this Article, the proposed *fact-based* fiduciary rationalization is likely capable of unravelling the Gordian knot of data misuse, given its flexibility and resonance with existing doctrine in both jurisdictions. If successful, this will promote better data practices *via* online service providers, particularly with the fourth industrial revolution surging ahead, with data as its essential fuel lighting the way.

390. GEORGE ORWELL, *1984*.
391. WILLIAM SHAKESPEARE, HENRY V act 1, sc. 1, ls. 45-47.