Indiana Law Journal

Volume 98 | Issue 2 Article 7

2023

Layered Fiduciaries in the Information Age

Zhaoyi Li
University of Pittsburgh, zhaoyi.li@pitt.edu

Layered Fiduciaries in the Information Age

ZHAOYI LI*

Technology companies such as Facebook have long been criticized for abusing customers' personal information and monetizing user data in a manner contrary to customer expectations. Some commentators suggest fiduciary law could be used to restrict how these companies use their customers' data.[1] Under this framework, a new member of the fiduciary family called the "information fiduciary" was born. The concept of an information fiduciary is that a company providing network services to "collect, analyze, use, sell, and distribute personal information" owes customers and end-users a fiduciary duty to use the collected data to promote their interests, thereby assuming fiduciary liability if it misuses or misappropriates customer data.[2] Although the possibility of an information fiduciary has generated significant attention, neither questions about the scope of the information fiduciary's duty of care nor whether corporate law's fiduciary duties are compatible with the information fiduciary duty have been satisfactorily answered.

In 2021, Facebook was renamed Meta Platforms, Inc., to expand business related to the Metaverse,[3] which is expected to bring about many new digital products. The establishment and development of the information fiduciary duty will help prepare the legal framework for this new era of digitization. This Article proposes a model to implement the information fiduciary's duty of loyalty and duty of care to end-users in today's information age by imposing these duties on Data Protection Officers (DPOs). First, this Article sketches the contours of information fiduciary duties on DPOs, examines how these duties can be structured, and clarifies how they interact with the duties owed by directors to the company. Second, this paper addresses the use of layered fiduciaries to alleviate the potential conflict caused by the information fiduciary duty. Third, this Article discusses in detail how the fiduciary duties imposed by Delaware corporate law can be applied to the field of digital privacy and consumer data. Directors' duties of care and loyalty in corporate law have developed over decades to form a useful system that is applicable in developing the information fiduciary duty. Implementing the information fiduciary duty can benefit from and be partially guided by existing law, like the director's duty to inform under

---

* Visiting Assistant Professor, University of Pittsburgh; J.S.D., Washington University in St. Louis. The author would like to thank Professor Danielle D'Onfro, Professor Scott Baker, Professor Robin Hui Huang, Professor Andrew Tuch, Professor Lauren Henry Scholz, Professor Amitai Aviram, Professor Asaf Lubin, Professor Daniel A. Crane, Professor Ryan Calo, Professor Rebecca Wexler, as well as the participants at the 2021 National Business Law Scholars Conference and 2022 Michigan Law Junior Scholars Conference for their thoughtful suggestions and valuable comments on an earlier draft of this Article. All mistakes are mine.

1. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016).

2. *Id.* at 1186, 1208–09 (introducing the concept of the information fiduciary and its uses).

3. *See Introducing Meta: A Social Technology Company*, META (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ [https://perma.cc/X96W-GDDP].

the duty of care and the duty to act in the best interests of the company under the duty of loyalty. Lastly, this Article explores how the information fiduciary duty can efficiently regulate multinational corporations' international data transfers, a rarely discussed yet important aspect of world economic development.

INTRODUCTION

Since most online services are provided without any charge,[4] who pays for their operations? Users foot the bill by surrendering their privacy,[5] with some commentators claiming "[d]ata is the new oil."[6] For example, insurance companies

4. *See* Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/ [https://perma.cc/C72A-9NYQ].

5. *Id.* Privacy includes not only personal secrets, but also personal information actively shown by users on social media. For additional explanation, see Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1192 (2017) ("One of the most common fallacies employed in our modern privacy discourse is the belief that once information is shared with others, it ceases to be private . . . .").

6. Kiran Bhageshpur, *Data Is the New Oil—And That's A Good Thing*, FORBES (Nov. 15, 2019, 8:15 AM), https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=1ecac3107304 [https://perma.cc/R8NJ-6BVP]; *see The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST, (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/FL4V-DP3S]. *But see* Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863, 864–65 (2019) (arguing that comparing data to oil is incorrect because it ignores the connection

can purchase data about users' mouse activity to detect Parkinson's, allowing them to increase premiums before users are diagnosed.[7] And internet companies like Facebook even collect data from non-users.[8]

Many corporations that provide online services earn their main revenue from advertising.[9] By providing content tailored to users' interests, Facebook strives to enhance user interaction, expose users to more targeted advertising, and capture more users' personal information.[10] Users' personal information helps companies infer preferences and tailor advertisements to the users' actual needs. The closer the fit, the more expensive the advertising fee.[11] The price of advertising products that align with user interests is higher than that for ordinary items of the same brand.[12] Therefore, Facebook prioritizes investing in groups responsible for increasing user numbers, data analysis, advertisement, and in-house counsel.[13] Some companies might win customers' favorable impressions by obtaining data and pushing customized information to users, thus improving user loyalty and ultimately increasing company revenue.[14]

---

between data and people).

7. Roger McNamee, *A Brief History of How Your Privacy Was Stolen*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/opinion/google-facebook-data-privacy.html [https://perma.cc/JU8T-M6JC].

8. Geoffrey A. Fowler, *There's No Escape from Facebook, Even if You Don't Use It*, WASH. POST (Aug. 29, 2021, 8:00 AM), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/ [https://perma.cc/FZF5-88Z2].

9. For example, advertising income accounted for 97.4% of Facebook's annual revenue in 2021. *See* S. Dixon, *Meta's (Formerly Facebook Inc.) Advertising Revenue Worldwide from 2009 to 2021*, STATISTA (July 27, 2022), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ [https://perma.cc/9BXR-N2D4]; *Meta's Annual Revenue (2010–2021, $ Billion)*, GLOBALDATA (June 2022), https://www.globaldata.com/data-insights/internet-services-social-media-technology-media-and-telecom/metas-annual-revenue/#:~:text [https://perma.cc/KR9X-GWLT]; Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the Internet*, N.Y. TIMES, https://www.nytimes.com/2021/09/16/technology/digital-privacy.html [https://perma.cc/ZBG3-5E8T] (Sept. 21, 2021).

10. *See* Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirringoutcry.html [https://perma.cc/4RNL-3XQW]; Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 12 (2020).

11. Greg Bensinger, *The Assault on Our Privacy Is Being Conducted in Private*, N.Y. TIMES (July 13, 2021), https://www.nytimes.com/2021/07/13/opinion/data-privacy-rights.html [https://perma.cc/R5S4-QFJC].

12. *See id.*

13. *See* Stephanie Stamm, John West & Deepa Seetharaman, *Is Sheryl Sandberg's Power Shrinking? Ten Years of Facebook Data Offers Clues*, WALL ST. J. (Oct. 1, 2021, 8:05 AM), https://www.wsj.com/articles/facebook-employee-data-zuckerberg-sandberg-olivan-11633089498?mod=article_inline [https://perma.cc/2P8A-EAXF].

14. *See* Shmuel I. Becher & Sarah Dadush, *Relationship as Product: Transacting in the Age of Loneliness*, 2021 U. ILL. L. REV. 1547, 1550 (2021) (describing how companies utilize big data to send accurately customized, warmhearted words to users to reduce users' safeguard ability and eventually influence users' interests).

In the information age—where profit is tied to personal data—users are exposed to risks. For example, users are put at risk if a dating website is not able to fulfill its promise of safeguarding users' personal information.[15] A company may provide users' personal information to advertisers that send them spam, or, as is often alleged, the company may not stop the spread of information used to manipulate elections or bring about war crimes, for example, in Tigray and Myanmar.[16] Users are willing to release their personal information to internet companies because most users lack sufficient knowledge about technology to thoroughly analyze the companies' behavior.[17] The small number of users who have the knowledge to understand how the company will use their information may be unable to distinguish what is a reasonable use pattern, let alone manage where their information is going.[18] Tech companies exploit users' blind trust and information asymmetry to use users' personal information. What makes this scenario worse is that many internet companies regard privacy issues merely as part of the corporations' compliance obligations to fulfill a series of checklists to avoid being sued.[19] Instead, the goal of privacy law should be to encourage companies to actively take measures to safeguard users' personal information.[20] The question guiding corporations' work should be "how can we proceed while creating fewer privacy risks for our consumers?" rather than "how can we prove compliance with the least disruption and risk to production?"[21]

---

15. *See, e.g.*, Andrea Peterson, *Ashley Madison Owner Agrees to Pay $1.6 Million to Settle U.S. Investigations*, WASH. POST (Dec. 14, 2016, 3:56 PM), https://www.washingtonpost.com/news/the-switch/wp/2016/12/14/ashley-madison-owner-agrees-to-pay-1-6-million-to-settle-u-s-investigations/ [https://perma.cc/77C8-7Z3M].

16. *See* Eliza Mackintosh, *Facebook Knew It Was Being Used to Incite Violence in Ethiopia. It Did Little to Stop the Spread, Documents Show*, CNN, https://www.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html [https://perma.cc/X6XC-YTY8] (Oct. 25, 2021, 11:25 AM); Aruna Viswanatha, *Facebook Ordered to Release Records on Closed Myanmar Accounts*, WALL ST. J., https://www.wsj.com/articles/facebook-ordered-to-release-records-on-closed-myanmar-accounts-11632360776 [https://perma.cc/9TPX-58DB] (Sept. 23, 2021, 9:10 AM).

17. *See* Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/CX5T-F7N9].

18. Balkin, *supra* note 1, at 1226–27.

19. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 778, 786, 800, 807, 820 (2020) (introducing the major changes in the field of users' privacy protection in recent years).

20. *See id.* at 776, 778 (critiquing the application of compliance in the personal information protection field as only focusing on the compliance process and ignoring the essence of protection).

21. *Id.* at 822; *see also* Jeff Horwitz, *The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It*, WALL ST. J. (OCT. 3, 2021, 7:36 PM), https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122?mod=article_inline [https://perma.cc/7YUF-EVH2] (revealing that Facebook is reluctant to instruct more employees to do things that would benefit users' safety when it may reduce engagement with their products).

As more and more privacy infringement cases have attracted public attention, corporations have realized the inevitability of regulation. Companies have changed their strategies, striving to pursue a regulatory model concentrating on compliance.[22] The focus of privacy protection has shifted from companies being bound by their own privacy policies to complying with regulations.[23] However, the reality is that even if the company employs officers who deal with privacy-related issues, it still may not achieve the desired outcome of protecting users' personal information.[24] As users' privacy awareness increases, more specific proposals are being brought to Congress, [25] which makes it possible to legally adopt further privacy protection schemes. This may play a role in promoting the protection of users' personal information. To safeguard privacy, elites in various industries are trying to find effective solutions to protect users' personal information with varying levels of short-term success.[26] For example, computer scientists are developing new products that allow users to own their data through blockchain, but when this online portal can be launched and applied in everyday life is unpredictable.[27] Entrepreneurs have established third-party companies, such as TrustArc, to issue privacy certificates for enterprises and guide companies to establish privacy guard frameworks,[28] but the possibility of websites with certification violating privacy policies is higher than that of websites without certification.[29] Legal scholars have proposed a scheme that is

---

22. *See* Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 23 (2021) (dividing privacy protection into two distinct waves).

23. *Id.* at 19, 22.

24. *Id.* at 22–23.

25. *See, e.g.*, Data Care Act of 2021, S. 919, 117th Cong. (2021) (requiring online platforms to (1) (A) "reasonably secure individual identifying data from unauthorized access", (B) "promptly inform an end user of any breach of the duty described in subparagraph (A) of this paragraph with respect to sensitive data of that end user."; (2) "not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user"); *see also Policy Principles for a Federal Data Privacy Framework in the United States: Hearing before the S. Comm. on Commerce, Science, and Transp.*, 116th Cong. (2019); *Consumer Data Privacy: Examining Lessons from the European Union's Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Science, and Transp.*, 115th Cong. (2018).

26. *See, e.g.*, Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333, 333 (2021) (proposing that the government set up a "public trust" to strengthen the regulation of personal information abuse).

27. Steve Lohr, *He Created the Web. Now He's Out to Remake the Digital World*, N.Y. TIMES (Jan. 10, 2021), https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html [https://perma.cc/5X3E-RUTY].

28. *Assurance and Certification Program Standards*, TRUSTARC, https://trustarc.com/consumer-info/privacy-certification-standards/ [https://perma.cc/3RTB-HZD3].

29. *Certifications and Site Trustworthiness*, BEN EDELMAN (Sept. 25, 2006), https://www.benedelman.org/news-092506/ [https://perma.cc/B95A-WAAQ]; Benjamin Edelman, *Adverse Selection in Online "Trust" Certification* (Harv. Bus. Sch. Working Paper, 2006) (on file with author), https://www.benedelman.org/publications/advsel-trust-draft.pdf [https://perma.cc/H2YX-3J6Z].

easier to implement in the short term. Namely, they have proposed the development of a unified information fiduciary duty as a stable foundation between network companies and users.[30]

The well-known legal notion of fiduciary duty is used widely in many industries. The Health Insurance Portability and Accountability Act (HIPAA) sets privacy standards within the medical field,[31] the Model Rules of Professional Conduct guide the privacy practices of lawyers,[32] and the Confidential Client Information Rule requires accountants to safeguard the confidential information of the party who receives their services.[33] Like other industries, online platforms should be bound by laws with similar privacy protection requirements.[34] Several scholars, such as Jack Balkin, suggest that tech platforms are fiduciaries and that they owe duties of care and loyalty to their users.[35] Under this proposed framework, private entities have the duty to prudently and faithfully act in the best interests of those who trust them.[36] In order to protect users' interests from damage, information fiduciaries who breach

---

30. *See* Balkin, *supra* note 1, at 1186. Other commentators hold similar views to Balkin. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 103 (2004); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 49 (2018) (providing several guidelines for enabling the information fiduciary duty to truly enter users' lives); *see also* Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 150 (2020) (clarifying that the distinction between Scholz and Balkin on information fiduciary duty lies in Scholz putting forward how information fiduciary duty applies to contracts with users' participation and applying information fiduciary duty to scenarios other than the First Amendment). Another proposal is to let an association undertake the fiduciary duty to protect users' personal information. For insight into this scheme, see Jaron Lanier & E. Glen Weyl, *A Blueprint for a Better Digital Society*, HARV. BUS. REV. (Sept. 26, 2018), https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society [https://perma.cc/9AGG-9CWP].

31. HIPAA Privacy Rule, 45 C.F.R §§ 160.101–160.552, 164.102–164.534 (2013).

32. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. (AM. BAR ASS'N 1983).

33. CODE OF PRO. CONDUCT pt. 1.700 (AM. INST. CERTIFIED PUB. ACCTS. 2014).

34. The differences between internet platforms and doctors and lawyers are that doctors and lawyers will analyze the personal information provided by patients and clients to customize the service type for them, while the platform does not have to know users' personal information in advance. In order to gain more economic benefits from users' information, digital corporations encourage users to disclose more information than they need to get free use of the application. Because doctors' behavior is closely related to patients' health, patients' privacy expectations for doctors are higher than internet users' privacy expectations. *See* Balkin & Zittrain, *supra* note 17; Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 517 (2019); Jack M. Balkin, *2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1229 (2017).

35. *See* Balkin, *supra* note 1, at 1186; *see also* Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CANADIAN BUS. L.J. 419, 458 (2001). Balkin's version of information fiduciary duty includes the duty of confidentiality in addition to the duty of loyalty and the duty of care. This paper does not discuss the duty of confidentiality in detail.

36. *See* Balkin, *supra* note 1, at 1207 (illustrating the roles and responsibilities of all parties in the fiduciary duty).

fiduciary duties are liable to data subjects.[37] However, the information fiduciary duty has aroused extensive debate. Some scholars believe that the information fiduciary duty of the company to users and the directors' fiduciary duty to the company will make various laws inconsistent.[38] Others reject this view, contending that no conflict exists between information fiduciary duties and those already imposed under corporate law.[39] In order to contribute to this debate, this Article proposes imposing information fiduciary duties on Data Protection Officers (DPOs), rather than companies. In doing so, this Article puts forward the concept of layered fiduciaries. A layered information fiduciary duty means that, in addition to the traditional fiduciary duty owed by directors and officers to their corporations and shareholders under corporate law, DPOs owe the duty of a layered information fiduciary duty to their end-users.

This Article proceeds in four parts. Part I briefly explains the information fiduciary debate, why the information duties can fill gaps in privacy law, the definition of layered fiduciaries, and how to implement the layered information fiduciary duty. Part II explores the boundaries of the duty of loyalty and duty of care in the layered information fiduciary context and examines the potential application of a layered information fiduciary duty in multinational corporations. Part III illustrates the role that corporate law can play in users' privacy protection and explores potential remedies.

I. THE INFORMATION FIDUCIARIES DEBATE

Those who support applying the information fiduciary duty to tech and social media companies argue that contract law does not adequately protect personal, private information from being misused by companies.[40] Lina Khan and David Pozen, opposing this view, believe that setting an information fiduciary duty to safeguard customer privacy presents a conflict with the duty to maximize shareholders' interests.[41] This leads to two distinct duties of corporations to both users and shareholders. Since these companies profit by selling their users' information, attempts to fulfill their informational fiduciary duty would violate their fiduciary duty to shareholders.[42]

---

37. For the definition of data subjects, see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 6, 2016 O.J. (L 119) 1, 33 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject') . . . .").

38. *See* Khan & Pozen, *supra* note 34, at 507, 509 (arguing that it is difficult to reconcile the contradictions between users and companies caused by the information fiduciary duty).

39. *See* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1908–11 (2021) (rejecting criticism that information fiduciaries' duties are irreconcilable with directors' and officers' traditional fiduciary duties); Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1008–11 (2022).

40. *See* Balkin, *supra* note 1, at 1227.

41. *See* Khan & Pozen, *supra* note 34, at 524 ("Balkin's proposal has the potential to swallow judicial dockets even with the aid of class actions, all while further undermining the defendant companies' ability to serve their shareholder beneficiaries.").

42. *See id.* at 508–09.

Directors, some of the main players in corporate law, provide a good illustration of how the fulfillment of separate fiduciary duties is not negatively affected by the existence of concurrent fiduciary duties owed to multiple parties.[43] To the extent there is a conflict, corporate law scholar Andrew Tuch rejects the notion that any conflict exists between corporate law and information fiduciary duties.[44] Like privacy law, environmental, consumer protection, antitrust, and criminal laws all restrict the maximization of shareholders' interests.[45] Yet these laws have all been successfully promoted and implemented. Privacy law should not be an exception.[46]

This Article partially agrees with Tuch's view that there is no conflict in the information fiduciary duty.[47] However, it is worth discussing and carefully considering the choice of the subject of the information fiduciary duty because choosing the appropriate subject is crucial. Choosing the wrong subject might not affect the implementation of this new concept in the short term, but it will affect the final performance and actual effect of the information fiduciary duty within each company in the long run. If the implementation of the information fiduciary duty fails to achieve users' expected reform effect due to the wrong choice of subjects, the results may be users' unemployment[48] and psychological pressure. In addition, users may no longer trust the technology companies' products. In the end, if the improper subject is chosen, this innovative new concept may only increase companies' operating costs and ultimately be abandoned. In order to prevent the practical problems that would arise if the company were chosen as the subject, this paper suggests using the concept of the layered information fiduciary duty with a focus on the role of DPOs. Like corporate directors strive to uphold traditional fiduciary duties to their corporations and shareholders, DPOs should uphold information fiduciary duties to users.

---

43. *See* Tuch, *supra* note 39, at 1922–23 (refuting scholars' criticism of the information fiduciary duty by using Goldman Sachs' directors as an example); DEL. CODE ANN. tit. 8, § 365 (West 2013) (requiring that directors owe a fiduciary duty to both stockholders and corporations).

44. *See id.* at 1911 (arguing the design of the information fiduciary duty model is ingenious: "[C]orporations face no conflicting fiduciary obligations since they would be bound by a single set of fiduciary obligations (to users). Directors are also bound by a single set of fiduciary obligations (to their corporation) . . .") (emphasis omitted).

45. *See* Balkin, *supra* note 10, at 23.

46. *See id.*

47. Tuch, *supra* note 39, at 1911.

48. For example, if the data about users' credit is wrong, it may cause users to be unable to find jobs. For a detailed explanation, see Yoni Blumberg, *Your Credit Report Can Keep You from Getting a Job—Here's How*, CNBC (July 2, 2018, 8:30 AM), https://www.cnbc.com/2018/06/29/how-your-credit-report-can-keep-you-from-getting-a-job.html [https://perma.cc/63CB-YCWG]; *see also* Elizabeth Gravier, *Can Employers See Your Credit Score? How to Prepare for What They Actually See When They Run a Credit Check*, CNBC, https://www.cnbc.com/select/can-employers-see-your-credit-score/ [https://perma.cc/A66G-JC3K] (Sept. 27, 2022).

A. The Concept of the Information Fiduciary Duty

1. Why Do We Need to Adopt the Information Fiduciary Duty?

The systematic and mature idea that the law should protect individual privacy originated in its modern sense in the nineteenth century,[49] but the true origin of privacy law can be traced to the series of constitutional amendments ratified to protect individuals from government invasions, such as the Fourth Amendment's protection against improper search and seizure.[50] However, traditional privacy laws, such as the Fourth Amendment, are insufficient for modern problems.[51] For example, if a private third-party internet company transfers users' data to the government, the law will not safeguard users' privacy.[52] The United States has not developed detailed constitutional and common law to regulate the behavior of private corporations that increase advertising revenue by arbitrary collection, collation, maintenance, use, analysis, cross-reference, disclosure, dissemination, synthesis, manipulation, and insecure disposal of digital consumers' personal data.[53]

Faced with tedious contracts, most users choose to consent to the privacy policy without reading it[54] because users understand that disagreeing with the privacy policy means that they cannot use the product. It is unreasonable to classify privacy law under the broad scope of contract law and rely on the limited and possibly vague terms of the contract to protect users' privacy from misappropriation.[55] Today, many companies avoid using the relatively more transparent "clickwrap" privacy policy in order to reduce their own risks.[56] Numerous digital businesses adopt the

---

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

50. U.S. CONST. amend. IV; *see also* U.S. CONST. amend. XIV.

51. For a fuller explanation of those exceptions, see Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 133 (2017).

52. *See* United States v. Miller, 425 U.S. 435 (1976). Since the information age requires more legal supervision of corporations, the entities of intruding users discussed in this paper are limited to corporations. As private entities, corporations can apply the information fiduciary duty and then summarize the experience to better promote it.

53. Manipulation has various forms. In addition to directly manipulating users, network platforms can indulge third parties by allowing them to manipulate users' rights for their own benefit. *See* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1100, 1102 (2019) ("[A]n information fiduciary framework should also address manipulation and discrimination in order to ensure that people are protected from the full array of modem digital threats that they face."). An information fiduciary duty can consider regulating behavioral advertising (advertising that needs to use virtual data archives to analyze users' interests) and allowing contextual advertising (advertising based on users' search content) techniques. For a fuller explanation, see Balkin, *supra* note 10, at 28.

54. *See* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014).

55. *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 993–94 (2021).

56. *See* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP.

"browsewrap" method, which lists the privacy policy on external internet sites and asks users to check voluntarily.[57] Some companies make it clear that privacy policies are not legal contracts, which makes it harder for such privacy policies to benefit users in the courts.[58] Courts have not consistently or precisely answered whether privacy policies are contracts.[59] Users are unlikely to get compensation based on contract law since it would take a lot of effort to prove the infringement of interests or determine the specific amount of compensation for the breach of a privacy contract.[60] Users and database operators sign form contracts directly. It is unrealistic and costly for the law to stipulate that all potential third-party corporations, such as advertising corporations and aggregator corporations who may have access to users' personal information, sign contracts with digital consumers and be responsible for users' privacy.[61] The contract would be limited because the data processor would affect the interests of non-users who do not legally constitute parties to the contract.[62] The difficulty of using contracts to protect users' personal information is also exemplified in the implementation of contracts between multiple companies handling users' personal information. Since data transmission is likely to involve more than two companies, companies need to make several contracts with different degrees of privacy protection between different parties, which may increase the workload of each company and result in difficulty in performing contracts.

Similarly, tort law also inadequately protects personal privacy needs in the contemporary information age. To be actionable under tort law, the plaintiff would have to suffer harm that "a reasonable person would find highly offensive,"[63] and the information may not relate to an issue of social focal points.[64] Tort law strictly examines whether there is "concrete injury," such as physical injury or economic

---

MEDIA & ENT. L.J. 181, 191 (2016) ("Under the clickwrap model, a website presents a user with the website's terms and requires that the user assent to those terms by clicking an icon . . . to signal her assent before using the website.").

57. *Id.* at 191–92 (describing the browsewrap agreement model).

58. *Id.* at 193.

59. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 807 (2022); *see, e.g.*, McGarry v. Delta Air Lines, Inc., No. CV 18-9827-MWF, 2019 WL 2558199 (C.D. Cal. June 18, 2019); Meyer v. Christie, No. 07–2230–JWL, 2007 WL 3120695 (D. Kan. Oct. 24, 2007); Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 45 (2019).

60. Waldman, *supra* note 19, at 812 (pointing out the practical difficulties encountered in court about the claim of privacy agreement); Norton, *supra* note 56, at 193 (illustrating why some courts refuse to equate privacy policies with contracts).

61. Balkin suggested that "privacy protections run with the data," and each company that can access personal information is not obligated to sign contracts with individual users. Balkin, *supra* note 1, at 1220.

62. *See* Balkin, *supra* note 34, at 1231.

63. Koeppel v. Speirs, 808 N.W.2d 177, 182 (Iowa 2011); *see, e.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809–10, 1849 (2010) (revealing that tort law emphasizes whether the severity of the facts of infringement meets the trial standard instead of examining the potential violation subject such as data players); RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

64. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

loss.[65] This view may devalue digital harm and lead to plaintiffs relying on minor actual damages to seek compensation rather than winning the case based on the core of the issue.[66] The typical causes of action in privacy torts, such as intrusion on seclusion, false light, and appropriation claims, are not adequate. For example, intrusion on seclusion is inadequate because the users' personal information obtained by the third-party data processing platform may not be first-hand data and does not infringe on an individual's domain.[67] It is also difficult for the plaintiff to win the lawsuit by depending on the false light cause of action because corporations might abuse users based on their real personal information.[68] In addition, it is futile to apply an appropriation claim to privacy litigation caused by database leakage.[69] Information fiduciary duties can make up for the shortcomings of traditional tort law because violating the information fiduciary duty constitutes actionable damage to users' trust in the company.[70]

Federal statutes also play a role in protecting users' privacy. However, federal laws, scattered across various fields, are not broad enough to effectively prevent all privacy violations by technology companies.[71] End-users are thus left in a vacuum, defenseless to privacy violations due to the absence of a holistic regulatory guideline.[72] For example, the Federal Trade Commission (FTC) does not allow corporations to use unfair and deceptive data, and private entities that violate their own privacy standards need to sign consent decrees to regulate their behavior.[73]

---

65. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2205 (2021); Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

66. For example, potential offenders can buy victims' residence information from information brokers' websites and physically injure victims. *See* Citron & Solove, *supra* note 59, at 832–33, 835. In fact, courts have not given equal treatment to the substantial injury caused by data collectors' disclosure of personal information and physical injury caused by the negligence of the property owner. *See id.* Meanwhile, there is a high chance that courts will be unwilling to recognize the financial losses in the cases involving personal information shared among multiple users. *See id.* at 826–27 (observing that the plaintiff who accused Apple of illegally collecting and using data through iPhone apps listed the loss of a place to store data as damage).

67. *See* Citron, *supra* note 63, at 1827 (enumerating various situations where traditional tort theory is not applicable to privacy law).

68. *Id.*

69. *Id.*

70. Richards & Hartzog, *supra* note 55, at 1012 (describing how the information fiduciary duty can bring realistic support to users in actual litigation).

71. STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 2 (2019) (pointing out that a scheme of federal regulations that can cover more areas is needed to meet the challenge of companies' invasion of users' privacy).

72. *Id.*

73. *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2018). "Deceptive" refers to a corporation failing to comply with its terms of service and deliberately misleading users. *Id.* "Unfair" refers to actions taken by companies that regulate the user's old personal information with the current privacy scheme, prevent users from easily canceling some unfavorable functions of certain software, or engage in behavior that might inevitably damage users' interests. *Id.* The FTC regulates deception more frequently than stricter fairness. *See* Schwartz & Peifer, *supra* note 51, at, 149–50. The FTC's cases can help other companies,

However, existing privacy law only deals with the processing of users' personal information itself and ignores the constraints on the complicated relationships existing in the information era.[74] It is not feasible to solve potential opportunistic conflicts, such as self-dealing, with the privacy governance rules implemented in today's age.[75] Furthermore, the FTC's approach includes one major loophole: corporations can draft the privacy agreements by themselves and simply change the details of their standard agreement to run contrary to user privacy expectations without being punished by the FTC.[76] Similarly, the FTC's privacy evaluation is not by their own examination and evidence collection, but rather is established by the testimony of corporations' own employees, giving the company the opportunity to provide a false story.[77] The FTC only governs users and corporations that have direct business dealings with users, but third parties who repeatedly step over the red line are not within the FTC's control.[78]

Moreover, the FTC cannot impose restrictions on the activities of airline companies, financial institutions, and other industries.[79] Additionally, the FTC has limited authority and discretion to issue meaningful remedies. For first offenders, the available remedy is limited to issuing a cease-and-desist order.[80] The FTC normally regulates corporate behavior through suggestions, exhortations, and warning letters instead of fines.[81] With years of practice, the FTC's broad-based standards have gradually narrowed into a governance tool for certain illegal actions.[82] Finally, the FTC handles only around ten cases every year,[83] which is far less than the users' demand for data protection, and even if a satisfactory decision is reached, the Supreme Court may eventually review and overturn the FTC's decisions.[84]

Other regulations focus on the infringement of consumers' personal information in certain fields. For example, the Gramm-Leach-Bliley Act (GLBA) safeguards the

---

especially tech platforms, to understand which type of activities will be regarded as unfair or deceptive. The FTC's cases are mainly resolved through consent decrees. If the decision is not accepted, the FTC can choose to file suits to request an injunction. For a fuller explanation, see MULLIGAN, FREEMAN & LINEBAUGH, *supra* note 71, at 31–32, 34, 58.

74. Richards & Hartzog, *supra* note 55, at 982.

75. *Id.* at 977–79 (discussing how modern privacy law is lacking).

76. *See* Dobkin, *supra* note 30, at 9–10 (criticizing the FTC for giving companies the opportunity to develop loose policies that are easy to obey).

77. Waldman, *supra* note 19, at 817 (discussing how Facebook lied to the FTC during its privacy assessment).

78. *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 107 (2020) (pointing out that the difference between the United States' and the European Union's approach to data regulation is that the European Union pays attention to the data itself, while the United States only ensures that the interests of users that are closely related to the data are not infringed).

79. Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2018).

80. *See id.* § 45(m)(1)(B).

81. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 212 (2016).

82. *See* Hartzog & Richards, *supra* note 39, at 1016 (listing some fixed types of violations of law regulated by the FTC).

83. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

84. *See, e.g.*, AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1352 (2021).

personal information of clients who purchase financial products,[85] the Health Insurance Portability and Accountability Act (HIPAA) imposes data protection obligations on patients' electronic medical data,[86] the Children's Online Privacy Protection Act (COPPA) ensures that children's online privacy will not be violated,[87] etc.[88] However, all of the above-mentioned regulations and some other acts, such as the Family Educational Rights and Privacy Act (FERPA), require individuals to first send their concerns to the relevant government agencies, such as the Family Policy Compliance Office or the U.S. Department of Health and Human Services Office for Civil Rights, rather than allowing individuals to sue corporations directly in court.[89] In addition, individuals are in a disadvantaged position due to the limited applicability of these statutes. For instance, although HIPAA concentrates on regulating patients' medical information and binds hospitals and medical practitioners' medical data use, HIPAA has no power to restrict insurers who also have access to individuals' health information.[90]

Considering that current privacy laws are unable to fully protect digital consumers' interests, some states have promulgated their own data protection-related laws. California enacted the California Consumer Privacy Act (CCPA) in 2020,[91] while Virginia will implement the Virginia Consumer Data Protection Act (VCDPA) in 2023.[92] However, these laws have great limitations. The VCDPA regulates recognizable users' data rather than the statistics commonly processed in practice.[93] In states with data protection laws, such as Virginia, cases can only be prosecuted by the state attorney general.[94] Even in the states where data subjects can sue corporations directly, the types of cases that can protect users' interests with privacy-related state laws are also limited. For example, Californians can only bring a suit against corporations for violating their data's safety based on the CCPA.[95] Therefore, divergent legislation in different states might result in users enjoying the same product with different privacy levels. It is necessary to formulate uniform, broader, and more detailed privacy-related laws to restrict the use and processing of personal information.

---

85. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

86. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

87. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended at 15 U.S.C. §§ 6501–06).

88. *See also* Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, §§ 601–22, 84 Stat. 1114, 1128–36 (1970) (codified as 15 U.S.C. § 1681); Video Privacy Protection Act (VPPA), Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as 18 U.S.C. § 2710).

89. *See, e.g.*, Davis v. Eagle Legacy Credit Union (*In re* Davis), 430 B.R. 902, 908 (Bankr. D. Colo. 2010); Lentz v. Bureau of Med. Econ. (*In re* Lentz), 405 B.R. 893, 899 (Bankr. N.D. Ohio 2009); Hudes v. Aetna Life Ins. Co., 806 F. Supp. 2d 180, 193 (D.D.C. 2011), *aff'd*, 493 F. App'x 107 (D.C. Cir. 2012); Lee-Thomas v. LabCorp., 316 F. Supp. 3d 471, 474 (D.D.C. 2018).

90. *See* Barrett, *supra* note 53, at 1069; 45 C.F.R. § 160.102(a).

91. CAL. CIV. CODE §§ 1798.100–1798.198 (effective 2018).

92. VA. CODE ANN. §§ 59.1-575–59.1-585 (2021).

93. *Id.* § 59.1-575.

94. *Id.* § 59.1-584.

95. CAL. CIV. CODE § 1798.150.

The European Union's General Data Protection Regulation (GDPR) also helps protect the personal information of American consumers.[96] Facebook founder Mark Zuckerberg once said that he hoped to require Facebook applications everywhere to comply with the strict standard of the GDPR.[97] Unfortunately, recent research shows that American companies use stricter operating procedures to deal with European Union users' personal information than their procedures for domestic users.[98]

Currently, U.S. privacy law focuses on whether users consent to non-negotiable privacy policies based on the user's real needs, which is consistent with individualism and democracy.[99] However, in reality, users are in a weak position in their relationship with network companies. Users are likely to click the "Agree" button quickly because they are unable to accurately process a large amount of information, or they are simply unwilling to read thousands of words in a limited timeframe.[100] When users agree to a technology company's privacy agreement, it is difficult for them to predict which aspects of their privacy rights will be violated by the company.[101] Almost all big technology companies collect users' data, so users do not have the option to opt out without foregoing services that almost everyone uses

---

96. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 6, 2016 O.J. (L 119) 1, 36 [hereinafter GDPR]. There are obvious differences in the degree of protection of users' personal information between the United States and Europe. European legislatures have endowed users with constitutional human rights to protect their personal information. Article 6 of the GDPR more strictly prohibits using users' personal information unless the use falls under one of a few exceptions. *See id.*; *see also* Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391, 397 ("Everyone has the right to the protection of personal data concerning him or her . . . . Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."); Schwartz & Peifer, *supra* note 51, at 127. In the United States, if relevant privacy law does not expressly restrict it, internet service providers are able to collect and use users' information. *Id.* at 135–36.

97. *See* Alyssa Newcomb, *Facebook Talks Nice but Takes Action as European Privacy Rules Loom*, NBC NEWS (Apr. 20, 2018, 3:22 PM), https://www.nbcnews.com/tech/tech-news/facebook-talks-nice-takes-action-european-privacy-rules-loom-n867856 [https://perma.cc/BNG4-RFYS]; Josh Constine, *Zuckerberg Says Facebook Will Offer GDPR Privacy Controls Everywhere*, TECHCRUNCH (Apr. 4, 2018, 4:26 PM), https://techcrunch.com/2018/04/04/zuckerberg-gdpr/ [https://perma.cc/2S6A-EQWM].

98. Jens Frankenreiter, *Cost-Based California Effects*, 39 YALE J. ON REGUL. 1068 (2022).

99. *See* Richards & Hartzog, *supra* note 5, at 1182 ("Thinking of privacy as an issue of personal choice, preferences, and responsibility has powerful appeal. It resonates with American ideals of individualism, democracy, and consumerism.").

100. Paying attention to internet users' consent to privacy agreements was learned from a similar scheme in the field of medicine, but the difference between these two scenarios is that consent in the medical practice generally comes from face-to-face communication. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/4LFW-ZNLX].

101. *See* Balkin, *supra* note 10, at 16–17 (describing the disadvantages of the notice-and-choice model).

in their daily life.[102] The GDPR alleviates these disadvantages by treating meaningless and non-actively initiated consent as void and unenforceable, allowing consent to be withdrawn,[103] ensuring users' access rights,[104] and charging large fines for collecting and improperly using user information.[105] Therefore, to improve privacy protection, the focus should shift from users to the real controller, corporations, who have more power to formulate the rules of the game in the information age.

The emergence of the information fiduciary duty can provide executive solutions for most of the above-mentioned, privacy-damaging behaviors. First, the information fiduciary model can allow ordinary people to sue corporations in courts to exercise their privacy rights in a real sense.[106] Private litigation rights allow the public to play a supervisory role and increase the possibility of successfully protecting their rights in real time. The right of individual users to bypass the attorney general and other government departments to directly file lawsuits in court, coupled with the relaxation of the requirement for users to prove that there is a clear link between the specific damage they have suffered and the company's invasion of their privacy rights, will ensure companies pay more attention to users' privacy in research and development and operation of online products.[107] Second, the control of personal information by the information fiduciary duty is not limited to a specific industry. This avoids the unsupervised use of user information in industries where regulations do not currently exist and the possible prevarication of management authority to different law enforcement departments. Third, under current law, privacy policy agreements may specify that disputes must be settled by arbitration, and the maximum compensation in arbitration is limited to the amount stipulated in the contract.[108] After the proposed reform, the company's failure to comply with the information fiduciary duty could be taken as a cause of action directly to the court, and the compensation would not be determined by the signed contract.[109]

Establishing an information fiduciary duty can also guide internet platforms' performance and prevent potential harm.[110] If the information fiduciary duty can be enforced, much can be changed or improved. For example, Facebook would be obliged to inform users if a third party is using their information. Users could opt to

---

102. *See* Dobkin, *supra* note 30, at 27 (recounting difficulties in eliminating discrimination towards users through data in real life).

103. GDPR, *supra* note 96, at art. 7; Ben Wolford, *What Are the GDPR Consent Requirements?*, GDPR.EU, https://gdpr.eu/gdpr-consent-requirements/ [https://perma.cc/T4QZ-YFE5].

104. GDPR, *supra* note 96, at art. 20.

105. *Id.* at art. 83; Wolford, *supra* note 103.

106. *See generally* Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639 (2022) (urging for individuals to have the right of private action to enhance the practical role of today's privacy law).

107. *See* Waldman, *supra* note 19, at 831–32 (2020) (recognizing that private rights of action would improve product quality).

108. *See* Scholz, *supra* note 30, at 196 (2020) (discussing how to apply the information fiduciary duty in various kinds of business in the market).

109. *Id.*

110. *See* Richards & Hartzog, *supra* note 55, at 968.

prevent the disclosure of their personal information to companies that might harm them, or they could oppose their measures through the pressure of public opinion.[111] It should be noted that the information fiduciary duty is not a panacea for all acts of abusing user information,[112] but it can greatly reduce marketing behaviors that manipulate consumers.[113] Even as technology evolves, the fundamental concept of the information fiduciary duty will still stably protect users' information from infringement without frequent modification of the law to adapt to the changes of the times,[114] which would otherwise drain legislative and judicial resources.

2. How to Implement the Information Fiduciary Duty to End-Users?

A new federal statute must be enacted that requires that DPOs owe an information fiduciary duty to users. Doing so will prevent companies from formulating different levels of privacy protection policies according to different laws of various states, which would result in an unequal user experience and protection of user rights. The law must also allow states to make slight differences in specific implementation and try different details according to their local conditions. Courts' detailed analysis and reasoning in upcoming landmark cases will help to build the details and trial standards of the information fiduciary duty. Case law will illustrate what is appropriate for companies to do under different circumstances, and corporations can, in turn, incorporate these standards into their code of conduct.[115] The information fiduciary duty should be compulsory. Some commentators suggest that corporations should choose whether to assume information fiduciary duties by themselves,[116] but

111. *See* Dobkin, *supra* note 30, at 46–47 (describing how a company could be sued for violating their privacy policies and how users could decide whether to share their information if privacy policies were comprehensible); Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/5LGF-D464].

112. *See* Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/YJ3R-9NAB] (suggesting that corporations should first analyze the concerns and seek advice from the FTC). Corporations should also share information on these potential risks with the whole society in a timely manner and help other companies avoid similar issues, and digital platforms that abide by such rules may not bear corresponding legal responsibilities. The difference between this proposal and compliance means that platforms adhere to clearly defined rules, whereas the proposed system requires engineers to be aware of and warn users of the possible misuse of their information. *See id.*

113. *Id.*

114. *See* Scholz, *supra* note 30, at 194 (discussing how the doctor-patient fiduciary duty is able to endure and adapt through changes in medical technology innovation and business models).

115. *See* Richard S. 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, 124–30 (2019) (putting forward a new scheme called "digital trustmediary" (DTM) and discussing other approaches to "data-centric business models" derived from the common law).

116. *See id.* at 108.

this is unlikely to succeed because most corporations pay more attention to short-term profits and stock growth instead of taking on additional duties to their users.

Commentators have also suggested that the information fiduciary duty of large corporations and small businesses should be different under common law because massive online shopping websites and small independent stores have different database sizes and abilities to manipulate users.[117] Although large corporations are the main target of the information fiduciary duty, this paper posits that legislation should not discriminate between companies based on size. Small companies, such as video surveillance start-ups and medical data processing start-ups, may cause the same or more serious harm as large companies. Small companies might not have developed compliance departments and a close connection between the industry and privacy, and the number of users affected by the infringement of small companies may not be as large as that of large corporations. However, the degree of injury for individual users of small companies is not necessarily smaller than that of large platforms. Small businesses with insufficient budgets can hire part-time, external, independent DPOs. The small number of users means that the salary cost of a part-time DPO is lower, and the risk of the DPO is smaller. Moreover, the penalty proposed in this Article is also determined according to turnover, so the amount of penalty borne by small companies' DPOs is small and bearable. However, authorities should make enterprises aware of the risk that sharing DPOs or employing DPOs with multiple positions might affect confidentiality.[118]

One core issue worth discussing is how to ensure that all companies appoint DPOs to implement the information fiduciary duty. The proposed information fiduciary law should require every company processing user data to have a DPO. DPO employment should be a prerequisite for the successful registration of new companies involved in processing users' data. Operating companies can be deterred by fines or reputation damages. In addition to the DPO requirement, company awareness of privacy protection needs to be expanded. Maybe some companies are unwilling to hire DPOs because it will increase extra operating costs. If companies realize that hiring DPOs will help to improve users' trust, thereby leading users to buy more of their products[119] and increasing the company's profits, more companies might hire DPOs even if there is no legal requirement.

The information fiduciary duty shall come into effect when users begin to use the company's service. DPOs do not need contracts to invoke fiduciary status, and the absence of such a written clause does not affect the fiduciary relationship's existence. The privacy agreement can be supplemented to specify that DPOs have the information fiduciary duty to end-users, but such supplemental clauses are not necessary. A layered information fiduciary duty will not affect the application of

---

117. *See* Richards & Hartzog, supra note 55, at 1008–10 (proposing to set the boundary between large and small companies).

118. *See Do I Need to Appoint a Data Protection Officer?*, RSI SEC. (Mar. 15, 2019), https://blog.rsisecurity.com/do-i-need-to-appoint-a-data-protection-officer/ [https://perma.cc/BN3X-HFSX].

119. Michael Fertik, *How to Get Customers to Trust You*, FORBES (Nov. 26, 2019, 2:43 PM), https://www.forbes.com/sites/michaelfertik/2019/11/26/how-to-get-customers-to-trust-you/?sh=26eb221f8d60 [https://perma.cc/8AKG-6KCX] (discussing a poll that found that eighty-one percent of customers say "trust impacts their purchasing decisions").

traditional professionals' fiduciary duty. For example, doctors in virtual telemedicine companies, such as Teladoc, that prescribe medication for patients or have artificial intelligence that provides a diagnosis, remain under HIPAA instead of the information fiduciary duty.[120]

B. The Intersection of Layered Information Fiduciaries and Corporate Law

1. What Is a Layered Information Fiduciary Duty?

Two scholars, Lina Khan and David Posen, believe that the corporate law theory that corporations must put the interests of shareholders first conflicts with the information fiduciary duty.[121] Allowing users to stay longer on online platforms would improve both corporations' and shareholders' profits.[122] On the other hand, prioritizing users' interests would make users less likely to expose their information, rendering corporations unable to accurately understand user preferences and tailor their services and advertisements accurately and attractively. Users' internet addiction might dissipate, and shareholders' earnings will be discounted accordingly. The same commentators argue that if the information fiduciary duty is implemented, corporate management will not be able to comply with their traditional fiduciary duty.[123]

The U.S. Supreme Court has explicitly stated that the notion that a corporation's sole purpose is to make a profit runs counter to today's corporate law:[124]

> While it is certainly true that a central objective of for-profit corporations is to make money, modern corporate law does not require for-profit corporations to pursue profit at the expense of everything else, and many do not do so. . . . So long as its owners agree, a for-profit corporation may take costly pollution-control and energy-conservation measures that go beyond what the law requires. A for-profit corporation that operates facilities in other countries may exceed the requirements of local law regarding working conditions and benefits. . . . Over half of the States, for instance, now recognize the "benefit corporation," a dual-purpose entity that seeks to achieve both a benefit for the public and a profit for its owners.[125]

---

120. *See* Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 40 (2020) (suggesting the information fiduciary duty learns from the framework of the trustee-beneficiary relationship).

121. *See* Khan & Pozen, *supra* note 34, at 504–07, 534 (discussing the difficulties of applying the information fiduciary duty to social media companies because these companies' fiduciary duties to shareholders and fiduciary duties to users conflict).

122. *Id.* at 505.

123. *Id.* at 504.

124. Burwell v. Hobby Lobby Stores, Inc., 573 U.S. 682, 710–11 (2014); Lynn Stout, *Corporations Don't Have to Maximize Profits*, N.Y. TIMES (Apr. 16, 2015, 6:46 AM), https://www.nytimes.com/roomfordebate/2015/04/16/what-are-corporations-obligations-to-shareholders/corporations-dont-have-to-maximize-profits [https://perma.cc/4VZS-5HP9].

125. *Burwell*, 573 U.S. at 711–13.

Are the types of companies mentioned by the court unwise? Why are the "benefit corporations" willing to spend time and money on things that do not bring direct monetary benefits? This may be because corporations realize that maximizing shareholder interests does not require sacrificing users' interests, and only pursuing the rapid growth of the corporation's profits may affect the future development of enterprises.[126] Users are willing to spend more time on online platforms with high integrity.[127] If a platform only focuses on how to make users' data generate higher profits, the users who care about their own privacy protection may choose to use other corporations' products.[128] Therefore, the relationship between the information fiduciary duty and directors' fiduciary duty to shareholders should not be regarded as conflicting. The long-term interests of users, society, corporations, and DPOs may harmoniously coexist.

Conflict arises when two sides have disagreements on certain things.[129] It should be recognized that conflicts between some legal provisions are truly inherent conflicts and may not be properly settled in an easy way within a short time.[130] For example, marijuana and medicinal use of marijuana are legal in nineteen and thirty-seven states, respectively,[131] but are not federally legal.[132] However, Tuch pointed out that the so-called conflict related to the information fiduciary duty is not necessarily true.[133] He illustrated that the subject of the information fiduciary duty is the corporation itself, while the subject of the traditional fiduciary duty in corporate

126. *See* LYNN STOUT, THE SHAREHOLDER VALUE MYTH: HOW PUTTING SHAREHOLDERS FIRST HARMS INVESTORS, CORPORATIONS, AND THE PUBLIC 63 (2012) (criticizing the traditional view about the corporations' purpose).

127. *See* Dobkin, *supra* note 30, at 11–12 (citing Miriam J. Metzger, *Privay, Trust, and Disclosure: Exploring Barriers to Electronic Commerce*, 9 J. COMPUTER-MEDIATED COMM. 00 (2004)).

128. *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 435 (2016); *see also* Waldman, *supra* note 19, at 809 ("Some privacy professionals and technology vendors . . . [s]ee privacy structures in marketing terms: users are more likely to continue to share information with data collectors if users feel their privacy is protected.").

129. For a fuller explanation of conflict in the context of a fiduciary duty, see Paul B. Miller, *Multiple Loyalties and the Conflicted Fiduciary*, 40 QUEEN'S L.J. 301, 304 (2014).

130. *See id.* at 304, n.10 ("An *actual* conflict is a situation in which the apparent interests of the relevant parties are presently in conflict. A *latent* conflict is a possible conflict that is inherent in a situation given factual or legal incidents of relationships between the relevant parties, the environment in which their interests will be pursued or protected, or the manner in which their interests will be pursued or protected . . . . Conflicts may be avoided as a result of changes in the interests of the parties, changes in the worldly circumstances in which they are (or were) interested, or through identification of decision options in which the incompatibility of interest between the parties is resolved.") (emphasis in the original).

131. *See* Michael Hartman, *Cannabis Overview*, NAT'L CONF. OF STATE LEGISLATURES (May 31, 2022), https://www.ncsl.org/research/civil-and-criminal-justice/marijuana-overview.aspx [https://perma.cc/5F2H-Z63U]; *State Medical Cannabis Laws*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 12, 2022), https://www.ncsl.org/research/health/state-medical-marijuana-laws.aspx [https://perma.cc/T8AL-UT24].

132. *See* Controlled Substances Act, 21 U.S.C. § 812(c) sched. I (c)(10) (listing marijuana as a Schedule I controlled substance).

133. *See* Tuch, *supra* note 39, at 1911–16.

law is the management team.[134] Although the company's commitment to the information fiduciary duty seems to make this idea noncontradictory, any problems in the company are still dealt with by directors and executives. Allowing qualified directors and executives to assume both responsibilities may make them hesitant because they will not know how to weigh their competing interests when making decisions and may approach the information fiduciary duty half-heartedly. They might feel that they are forced to formulate specific rules relating to the information fiduciary duty within the company in order to comply with the law. They may try to design the rules solely with profits in mind at the expense of users' privacy interests. Unqualified directors and executives who only care about their corporation's economic interests might rely on profits as an excuse for them to completely ignore their duties to users. None of these scenarios are ones that the proponents and improvers of the information fiduciary duty want to see.

This paper argues that DPOs, instead of companies, should take the information fiduciary duty and fulfill their duty of care and duty of loyalty to end-users. DPOs are individuals who can initiate the decision-making process by themselves, and their work includes actively understanding relevant laws and technologies and making substantive efforts to avoid abuse of users' personal information.[135] This work content makes them more suitable candidates for holding the information fiduciary duty than companies that are not experts in the data protection field. Currently, DPOs are composed of experienced experts from various fields,[136] but the responsibilities and duties of DPOs are not clear enough. Giving DPOs more practical responsibilities, such as the information fiduciary duty, will give them more power and voice, which increases the significance of hiring DPOs. Because companies might regard profit as their most urgent priority, it is better to give the information fiduciary duty to DPOs who are in a better position to serve the interests of the user.

This new DPO position created in the information age meets the needs of all aspects of the information fiduciary duty. If the company itself were to take the role of the information fiduciary duty, it may choose to shield or cover its misconduct; but if DPOs bear the information fiduciary duty, there is a greater probability that the DPO will not hide the company's abuse of users' personal information from society. At minimum, the DPO would supervise the company in correcting relevant wrong behaviors in a timely manner. This means that DPOs can take measures to make the company more profitable without impacting users negatively, and if the

---

134. *See id.* at 1909–10 (clarifying the implementation object of the fiduciary duty in corporate law); *see also* Alessi v. Beracha, 849 A.2d 939, 950 (Del. Ch. 2004).

135. The EU has explained the responsibilities of DPOs. For a fuller explanation, see Eur. Data Prot. Supervisor, *Data Protection Officer (DPO)*, EUROPA, https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en [https://perma.cc/4SG2-HL7H].

136. *See* Gary Beach, *GDPR Is Almost Here, Let the Data Protection Officer Talent Race Begin*, WALL ST. J. (Mar. 1, 2018, 11:03 AM), https://www.wsj.com/articles/gdpr-is-almost-here-let-the-data-protection-officer-talent-race-begin-1519920221 [https://perma.cc/5NZE-QQPG] ("Career paths leading to a data protection officer position are not discernible. A review of 20 data protection officer profiles on LinkedIn found 35 percent came from IT, 30 percent were lawyers, 20 percent were security professionals and 10 percent had compliance backgrounds.").

company tries to be profitable at the expense of users, DPOs are able to offer solutions that balance data protection and data use.

The proposed layered fiduciary concept involves a corporate law adoption of the layered, non-parallel information fiduciary duty at the theoretical level. This means that the DPOs have the information fiduciary duty to users on one layer, and directors and executives have the fiduciary duty to the company and shareholders on the other. The establishment of the layered information fiduciary duty is not only necessary for users but also beneficial to the growth of the corporations' long-term interests. Imposing the information fiduciary duty on DPOs will move the debate about the information fiduciary duty forward and will provide a theoretical basis for the court to apply in information fiduciary cases.

Imposing the information fiduciary duty on DPOs promotes corporate social responsibility (CSR) and environmental, social, and corporate governance (ESG), which is conducive to the long-term interests of the company. Corporations that attach importance to CSR make efforts to go beyond industry standards. For example, corporations may increase product quality inspection, discharge sewage and waste gas after filtration, and take the interests of stakeholders, such as vendors and workers, into account when making decisions.[137] CEOs of many large corporations have promised to consider stakeholders' interests,[138] and some states even stipulate that directors may examine the factors related to CSR when dealing with corporate affairs.[139] CSR comprehensively summarizes the company's dedication to stakeholders' interests, while ESG is a set of specific quantitative assessment standards to help improve the company's sustainable development.[140] The effective operation of CSR and ESG helps DPOs eliminate possible resistance from the corporate level.

Because the corporate governance mechanism accommodates divergent interests, such as shareholders' interests and stakeholders' interests, an opening is left for the implementation of information privacy law. The fiduciary duty to shareholders in corporate law and the layered information fiduciary duty in privacy law can coexist in the layered fiduciary theory. The managers and DPOs discuss the specific degree of balance according to the actual situation, and corporate law does not need to specify which layer has priority.[141] In order to better implement the information fiduciary duty, industry experts can release some basic versions of the implementation process of the information fiduciary duty in meetings related to privacy law. This guide may include the implementation process of training

---

137. *See* Li-Wen Lin, *Corporate Social Responsibility in China: Window Dressing or Structural Change?*, 28 BERKELEY J. INT'L L. 64, 64 (2010).

138. *See Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans'*, BUS. ROUNDTABLE (Aug. 19, 2019), https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans [https://perma.cc/PZ66-TA4N].

139. *See, e.g.*, CONN. GEN. STAT. § 33-756(g) (2018).

140. *See* Thomas Lee Hazen, *Corporate and Securities Law Impact on Social Responsibility and Corporate Purpose*, 62 B.C. L. REV. 851, 854 (2021).

141. *But see* Tuch, *supra* note 39, at 1917 (arguing that the information fiduciary duty should be met first since compliance with the law is the priority of the company).

engineers on user privacy in product design, the duty of care in data collection, and much more. DPOs can follow the instructions and set a fixed, specific process for the information fiduciary duty's implementation according to the specific situation of the company, and all personnel involved should follow this scheme and provide due support. If a lawsuit arises, the court can pay attention to whether the formulation of the process is standardized and whether DPOs do their work according to the process. At the same time, the court can gradually clarify the DPOs' best practices in specific circumstances. In addition, corporate law can also consider advocating "abstract corporate purposes,"[142] which can take stakeholders' interests into account, rather than just fulfilling the fiduciary duty to shareholders to maximize their interests. Only by taking multipronged measures can companies effectively protect users' interests.

2. Comparing the Layered Information Fiduciary Duty and Corporate Law's Fiduciary Duties

The fiduciary duties between directors and corporations and between doctors and patients are not exactly identical to those between DPOs and users.[143] Specifically, they differ in two ways. First, the layered information fiduciary duty is stricter and more detailed since it is a brand-new concept and lacks best practice guidance. In contrast, the concept of traditional fiduciaries, such as corporate directors and lawyers, is familiar to the public, has been mature for many years, and the court has set up many best practice cases to follow. If the new concept sets a loose standard for the layered information fiduciary duty at the beginning of implementation,[144] there will be no significance in setting it. Therefore, the layered information fiduciary duty should use the most accurate language to describe every possible circumstance, so that the company cannot circumvent its application. Delaware corporate law, for instance, stipulates that the directors have a fiduciary duty to the shareholders and corporations.[145] The layered information fiduciary duty requires DPOs to have the duties of care and loyalty to users. There is no conflict between these two duties because the subjects of the fiduciary duty are different.[146]

---

142. Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 586 (2015) (proposing that directors can pursue the company's abstract purpose).

143. *See* Khan & Pozen, *supra* note 34, at 506–07 (2019) ("[W]hile digital information fiduciaries would not be unique in facing crosscutting fiduciary obligations, the nature and scope of the conflicts they would face seem qualitatively distinct."); Tuch, *supra* note 39, at 1916.

144. *See, e.g.*, DEL. CODE ANN. tit. 8, § 102(b)(7) (2021) ("A provision eliminating or limiting the personal liability of a director to the corporation or its stockholders for monetary damages for breach of fiduciary duty as a director . . . .").

145. Quadrant Structured Prods. Co. v. Vertin, 102 A.3d 155, 171 (Del. Ch. 2014) ("The directors of a Delaware corporation owe fiduciary duties to the corporation they serve."); Skeen v. Jo-Ann Stores, Inc., 750 A.2d 1170, 1172 (Del. 2000) ("Directors of Delaware corporations are fiduciaries who owe duties of due care, good faith and loyalty to the company and its stockholders.").

146. Tuch, *supra* note 39, at 1911 ("Under Balkin's proposal, it is readily apparent that *corporations* face no conflicting fiduciary obligations since they would be bound by a single set of fiduciary obligations (to users). *Directors* are also bound by a single set of fiduciary

What these duties have in common is that they influence decision-making. The directors provide advice and make decisions on major matters of the company, and DPOs provide suggestions and make decisions about user privacy. Meanwhile, directors may have more information and higher business skills than the company, which might cause the company to be damaged by directors due to unequal information. This inequality of information is also reflected between DPOs and users. For example, if it were not exposed by the media, ordinary users of the Ring doorbell app would have no knowledge of the fact that third parties secretly obtained their IP addresses.[147] It is these similarities that make the basic contents of the traditional fiduciary duty and the layered information fiduciary duty roughly correspond to each other.

II. A PROPOSAL FOR A WORKABLE MODEL OF LAYERED INFORMATION FIDUCIARIES

Implementing an idea into practice requires the support of a detailed implementation mechanism for guidance. Section II.A identifies three categories of the layered information fiduciary duty's duty of care and duty of loyalty, respectively.[148] Clear, substantive guidelines for the content of information fiduciaries will enable judges to have a plain basis when ruling on a case.

A. How Can the Fiduciary Duties in Corporate Law be Transformed into the Layered Information Fiduciaries?

This Section will outline the parameters of the layered information fiduciary duty by reviewing the fiduciary duty of directors in corporate law. The directors' fiduciary duty has a long history and has formed a relatively stable and mature system after fifty years of academic discussion by scholars and repeated practice in the industry. Therefore, directors' fiduciary duty under corporate law is a good source for constructing what should be included in the layered information fiduciary duty.

1. Duty of Care

Because it is executed with less strength and is afforded less attention, the duty of care appears to be less important than the duty of loyalty for directors.[149] However, the regulation and implementation of detailed guidance within the duty of care are important for the protection of user information. The current literature and laws lack detailed explanations and analysis of the various types of the information fiduciary's

---

obligations (to their corporation) . . . .") (emphasis in the original); *see also id.* at 1921–24.

147. *See* Bill Budington, *Ring Doorbell App Packed with Third-Party Trackers*, ELEC. FRONTIER FOUND. (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers [https://perma.cc/7KDV-QERC].

148. It should be noted that the classification of the information fiduciary duty should be dynamic in the long run. The current version is based on today's needs. In the future, if there are new needs for information fiduciary duties, the current version should be supplemented to ensure new cases have laws to rely on.

149. Julian Velasco, *A Defense of the Corporate Law Duty of Care*, 40 J. CORP. L. 647, 648 (2015) (pointing out that the duty of care receives less respect than the duty of loyalty).

duty of care and how these duties are applied.[150] This absence of guidelines may affect the application of the layered information fiduciary duty and cause overreliance on the duty of loyalty. A clarified typology of the layered information fiduciary duty would guide the behavior of service providers and clarify liability. Generally, the duty of care requires directors to do their best to supervise the operation of the corporation,[151] investigate and inquire about relevant corporate affairs in a timely manner,[152] and "make reasonable decisions" in a correct way.[153] The design of the layered information fiduciary duty's duty of care can refer to the application of this content to specific privacy scenarios.

To achieve meaningful privacy protection, it is a best practice to raise privacy issues and formulate privacy agreements in compliance with one's layered information fiduciary duty while designing products.[154] If platforms start to solve the potential problem of violating users' privacy in the limited time before the product is ready to be put on the market, users will face great risks.[155] The constituent parts of the layered information fiduciary duty would be both prescriptive and proscriptive.[156] Prescriptively, the duty of care would encourage companies to follow the highest standards and strictly command themselves. The duty of loyalty can focus on proscriptive principles, enabling the company to intuitively understand what behavior is not acceptable. Specifically, the duty of care under the information fiduciary duty includes three parts. First, the directors shall take efficient measures to keep track of their companies' business and promptly understand the first-hand data obtained by the board. [157] This means that a conscientious director of an internet company should have a basic understanding of how the company collects and uses users' personal information and deals with potential information misuse or data breaches in a timely manner, given that this may affect the company's reputation and stock price. This timeliness requirement is reflected in the layered information fiduciary duty in several ways. First, DPOs shall ensure that the company's specific algorithms for collecting, collating, copying, using, storing, organizing, transferring, translating, disclosing, or making derivatives about personal information shall be changed in time with updates to their privacy policies. If the privacy policy changes, users need to be informed in real time. Unreasonable delay might harm users'

---

150. A congressman submitted a bill, The Data Care Act, regarding the information fiduciary duty, but it was not passed and lacked detailed substance. *Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online*, BRIAN SCHATZ: U.S. SENATOR FOR HAW. (Dec. 12, 2018), https://www.schatz.senate.gov/news/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online [https://perma.cc/P8NT-A4RR].

151. MODEL BUS. CORP. ACT ANN. § 8.31(a) cmt. 1(F) (2020).

152. *See* Melvin A. Eisenberg, *The Duty of Care of Corporate Directors and Officers*, 51 U. PITT. L. REV. 945, 948 (1990) (enumerating several aspects of directors' duty of care).

153. *Id.*

154. *See* Waldman, *supra* note 19, at 785 n.71; *see also, e.g.*, GDPR, *supra* note 96, at art. 25.

155. *See* Waldman, *supra* note 19, at 785 n.71.

156. Miller & Gold, *supra* note 142, at 547–48.

157. Eisenberg*, supra* note 152 (summarizing what types of duty of care directors should carry out).

interests because users may need to adjust the cookie permissions settings according to the adjustment of the protocol. The purpose of setting a privacy agreement should be to allow users to be aware of the whole process of how the company uses users' privacy information, rather than trying to make users click the "I agree" button faster.[158] Second, DPOs shall promptly detect the risk of data leakage and diligently try to protect users' data security. The specific implementation measures can be reflected in software engineers' induction training, educating engineers to regularly check the security of users' personal information and retraining software engineers who fail to fulfill the layered information fiduciary duty in product design. Since many data leaks are caused by employees,[159] DPOs should establish a reporting mechanism to gather direct information faster. Third, DPOs should arrange for engineers to establish a fixed process to allow users to update and supplement their personal information regularly. They should also urge the third-party information processing organization to timely provide feedback on outdated or inaccurate user information and communicate with the user in a timely manner. The reason for this is that outdated information may negatively affect the user experience.

Second, the construction of the layered information fiduciary duty is inseparable from one of the core components of the duty of care—the duty to inform. There are two requirements for directors' duty to inform: understanding the company's daily progress and ensuring that their choice is based on all relevant, obtainable information. [160] Qualified and experienced directors will actively acquire and understand corporations' operational plans.[161] A director can keep informed of their company's business by attending board meetings in person, listening to reports and opinions from experts, and signing financial statements. The duty to inform is essential to the directors' role because it ensures they are fully aware of the company's happenings, enabling them to make wise decisions. *Francis v. United Jersey Bank* explained that "[d]irectors may not shut their eyes to corporate misconduct and then claim that because they did not see the misconduct, they did not have a duty to look. The sentinel asleep at his post contributes nothing to the enterprise he is charged to protect."[162] Accordingly, there are two layers of duty to

158. *See* Leif-Nissen Lundbæk, *Kill the Standard Privacy Notice*, TECHCRUNCH (July 6, 2021, 9:08 AM), https://techcrunch.com/2021/07/06/kill-the-standard-privacy-notice/ [https://perma.cc/RF8U-SC62].

159. *See* Symposium, *Fall 2016 Cross-Border Data Privacy Issues*, 25 CARDOZO J. INT'L & COMP. L. 379, 387 (2017).

160. *See* Eisenberg, *supra* note 152, at 952, 958; Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985) ("The determination of whether a business judgment is an informed one turns on whether the directors have informed themselves 'prior to making a business decision, of all material information reasonably available to them.'") (quoting Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984)); *Aronson*, 473 A.2d at 812 ("[D]irectors have a duty to inform themselves, prior to making a business decision, of all material information reasonably available to them. Having become so informed, they must then act with the requisite care in the discharge of their duties.").

161. *See* Cede & Co. v. Technicolor, Inc., 634 A.2d 345, 368 (Del. 1993); *see also* Francis v. United Jersey Bank, 432 A.2d 814, 822 (N.J. 1981) ("Directors are under a continuing obligation to keep informed about the activities of the corporation. Otherwise, they may not be able to participate in the overall management of corporate affairs.").

162. 432 A.2d at 822.

inform for DPOs under the layered information fiduciary duty. One is to fully inform users, and the other is to fully inform companies when dealing with privacy matters. Ideally, users will have a clear way to learn which corporations and which employees are using their personal information, and how they are using it.[163] Specifically, users should be informed of the municipal location of employees who have access to the data; the types of data collected; and the reason for its collection, such as market analysis, advertising, or sale to data brokers, and other reasons.

At no point can DPOs satisfy their duty to inform simply by requiring users to sign a generic privacy agreement. The following describes what DPOs must do to fulfill their duty to inform users. In order to make this Section more specific and operable, the duty to inform can be divided into three periods: before collecting users' personal data, while using the data, and after using the data.

Before collecting data, DPOs should urge engineers and the legal compliance department to inform users, using plain language, of what information they intend to collect, why they are collecting it, how long they will retain the data, who will have access to it, whether the data will be encrypted, what risks users face when disclosing their data, and what to do in the event of unauthorized disclosure, hack, or data loss. In 2020, Zoom breached their duty to inform by pairing Zoom users with their LinkedIn page. Users who paid for this capability could view the personal LinkedIn information of other users, such as their work experience and educational background, without their knowledge.[164] Under these facts, had the proposed regime been in place, Zoom's DPO would have violated its layered information fiduciary duty to users.

While utilizing users' personal data, DPOs must ensure that engineers' use of personal information is consistent with the information provided to users. A counterexample would be Google continuing to actively obtain and transmit users' geographic information and keep user records through various channels and other software companies for their own interest, despite users explicitly rejecting such behavior through their privacy settings.[165] Anonymously web searching does not guarantee that the user's browsing records and preferred topics remain secret.[166] Regardless of whether engineers intentionally or unintentionally collect this information, these actions should be regarded as a violation of the duty of care under the proposed layered information fiduciary duty. If DPOs want to avoid their companies crossing these red lines, the best practice is to regularly and comprehensively disclose pertinent information, provide users with user information protection reports on a quarterly basis, and describe substantive efforts to ensure privacy protection. DPOs should regularly train engineers on the duty to inform

---

163. *See* Whitt, *supra* note 115, at 104.

164. Aaron Krolik & Natasha Singer, *A Feature on Zoom Secretly Displayed Data from People's LinkedIn Profiles*, N.Y. TIMES, https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html [https://perma.cc/C2YC-TSGX] (Oct. 14, 2021).

165. *See* Greg Bensinger, *Google's Privacy Backpedal Shows Why It's So Hard Not to Be Evil*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/14/opinion/google-privacy-big-tech.html [https://perma.cc/9F8R-2U82].

166. Jennifer Korn, *Private Browsing May Not Protect You as Much As You Think*, CNN BUS., https://www.cnn.com/2022/07/23/tech/private-browser-security/index.html [https://perma.cc/C2UB-JX57] (July 25, 2022, 8:31 AM).

requirements so that those who handle user information understand best practices. In addition, DPOs should effectively remind engineers to always ensure the confidentiality and accuracy[167] of personal information,[168] quickly notify users when hackers attack or accidental data leaks occur and disclose information about the leak's damage and recommended mitigation strategies.

After the company collects data, DPOs shall supervise the platform, inform users of the flow of their personal information, and issue detailed reports to users. Users' personal information can be classified according to its importance and the degree of impact on users. The importance of the duty to inform should be calibrated to the quantity and quality of information. DPOs should enable users to control and prevent their personal information from going to places the user does not wish it to go. Timely notification to the user will give the user the opportunity to modify data inaccuracies, prevent the company from collecting the data, or prohibit the company from using the data. If users find information illustrating that the company has no right to keep personal information beyond the scope stipulated by law, users will have time to prepare for the potential consequences. If the company fails to comply with digital consumers' expectations, the transfer of users' personal information between subsidiaries would constitute a breach of the layered information fiduciary duty.[169] For example, end-users should be informed about any sharing of their personal information with third-party companies, including subsidiaries. Layered information fiduciaries are only permitted to share information with third parties after obtaining users' direct and explicit consent in advance.

To solve the problem of users choosing not to read data collection reports with large amounts of information, scholars have proposed personalizing the content.[170] Users can be encouraged to fill out questionnaires, write down their concerns in advance, and identify what they want the company to disclose to ensure their privacy rights and interests are protected in the manner they expect. Corporations may be unwilling to inform users of how their information is processed because they are afraid that users will restrict access to their personal information after understanding what it is used for, resulting in damage to online platforms' economic interests.[171] Therefore, DPOs, who are relatively independent and have interests aligned with users, undertake the information fiduciary duty, greatly reducing the risks faced by users.

---

167. Inaccurate personal information such as incorrect or fabricated criminal records may make it difficult for job seekers to find employers.

168. Several commentators endorsed the idea that the duty of confidentiality should exist independently from the duty of care and the duty of loyalty. However, the author thinks that the core element of the confidentiality duty can be classified under the duty of loyalty. *See e.g.*, Balkin, *supra* note 10, at 14 (articulating the three components of the information fiduciary).

169. *See* Dobkin, *supra* note 30, at 38 (explaining what behavior of the subsidiary will breach the information fiduciary duty).

170. *See* Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1417 (2014).

171. Marcus Moretti & Michael Naughton, *Why Privacy Policies Are So Inscrutable*, ATLANTIC (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/ [https://perma.cc/8FSX-8YCZ].

In addition, it is an important requirement of corporate law for a director to be fully informed in specific circumstances, such as when approving certain transactions.[172] In the process of dealing with privacy issues, DPOs will also make many decisions that may greatly influence users' privacy protection. The layered information fiduciary duty can standardize the decision-making process to guarantee the safeguarding of end-users' interests. When DPOs make decisions on privacy issues—such as whether to warn engineers who collect personal information without giving users other options or allowing users to destroy all personal information when they close their accounts; whether to guide engineers to maintain and process users' records correctly; whether to advise engineers to request users' permission more often; and whether to report that the platform enables privacy related functions such as face recognition by default instead of waiting until the users opt in to such services—DPOs would not only ensure that the platforms inform users, but also make platforms aware of the consequences of their actions.

Third, under corporate law, the director's duty of care includes adequate inquiry, making decisions conducive to the corporation's development, and supervision of the corporation's operations.[173] The Model Business Corporation Act stipulates that directors can act on lawyers' and accountants' advice.[174] Accordingly, DPOs should represent users' interests when dealing with third parties such as marketing partners and advertisement companies. DPOs have the right to inquire about how third parties use personal information, evaluate whether the third party is qualified to protect users' information, and make decisions for their users, including advising companies to terminate contracts with third-party companies that harm their users' interests. Although companies are allowed to provide users' data to other platforms, DPOs can supervise and urge online companies to limit the level of personal information that can be provided in the agreement, and they can be cautious when sharing users' sensitive information such as their religion, race, and sexual orientation. DPOs should also ensure that the privacy policy specifies the procedures for use of personal information,[175] which will be helpful for users to understand how their personal information is processed. Adequate care for users should also include reasonable and appropriate reliance on third-party companies, ensuring that third-party companies cannot access personal information without users' consent,[176] supervising the third party who has users' consent, ensuring users retain a right to withdraw their consent and data, and protecting the users' data carefully.

---

172. *See* Eisenberg, *supra* note 152, at 958 (providing a specific guideline for directors' duty of care).

173. *See id.* at 948; MODEL BUS. CORP. ACT ANN. § 8.31(a) cmt. (1)(E) (2020) ("The director's role involves two fundamental components: the decision-making function and the oversight function . . . . Also embedded in the oversight function is the need to inquire when suspicions are aroused.").

174. MODEL BUS. CORP. ACT ANN. § 8.30(f) (2020).

175. *See* Dobkin, *supra* note 30, at 44 (refining the common characteristics of privacy policies of large corporations such as Walmart, Uber, Google, and Facebook).

176. The third party may access users' data without utilizing the digital corporations' data sharing. Cookies may be installed by a third party under the authorization of the platform. For an analysis regarding third parties, see Balkin, *supra* note 10, at 14–15.

If the third party has recently been punished by relevant authorities, such as the FTC, for violating user privacy, DPOs should reasonably doubt the third party's qualifications and should take this into account when deciding to do business. DPOs should spot check whether third parties collect users' personal information for the agreed reason or for reasons beyond their operational purposes. DPOs must also timely supervise and urge third parties to find and fix security gaps. The directors' fiduciary duty mechanism does not require directors' direct supervision of third parties.[177] DPOs can ensure the implementation of supervision by formulating clear supervision processes and evaluation guidelines.

A possible scenario involving third parties occurs when one company needs to turn over users' personal information to another company in a merger. DPOs shall ensure companies inform the users of where their personal information is going in advance and supervise the third-party company to ensure user privacy agreements are re-signed so that the third party's DPO becomes the users' information fiduciary. It is important to inform users of the identity of the third parties that will use or collect their personal information and how they will use that information because most nonprofessional users lack sufficient knowledge to quickly identify third party companies' names and business areas. In order to avoid sharing data with a third party that may manipulate users, DPOs can assign an internal team to understand what the third party intends to do with the shared data in detail, including if and how it will be used for research. DPOs must regularly organize audits to ensure the third party is using users' personal information for only the agreed purposes rather than unrelated purposes. Although the majority of platforms transmit unidentified data to third parties, third parties can still recognize the user's identity through decryption.[178] For example, analyzing an individual's data from their Netflix account and public information on IMDB.com at the same time would enable a third party to reestablish identifying information.[179] If a third party uses personal information illegally or divulges it, DPOs should ask platforms to terminate their relationships with that third party and resecure their users' personal information in a timely fashion.[180]

To be clear, any collection of users' personal information without their consent infringes on user privacy, regardless of whether that data is shared with third parties. Collecting information in a manner that violates the layered information fiduciary duty would impair end-users' degree of control and affect users' ability to determine the broadcasting range of their data.[181] Users will then be unaware of potential future risks to their privacy, especially when users have already deleted an app or have forgotten to use it, let alone be able to arm themselves in advance to prepare for possible risks.

Third parties include various companies of different types and sizes, such as marketplace sellers and platforms that specialize in tracking and analyzing.[182] Advertising firms are not appropriate third parties with which to share users'

177. *See* Eisenberg, *supra* note 152, at 952.

178. *See* Moretti & Naughton, *supra* note 171.

179. *Id.*

180. *See* Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2052 (2018).

181. *See* Citron & Solove, *supra* note 59, at 853–54.

182. *See* Dobkin, *supra* note 30, at 38–39.

personal information. The advertising company should not directly share personal information with the tech platform but should provide the platform with the appropriate consumers for their product.[183] The online platform can then display advertisements to the appropriate population that is likely to purchase the product.[184] This process helps control the initial spread of data and reduces the risk of data leakage and unauthorized access. Mysterious aggregator companies can be third parties that collect users' uniquely identifiable information including purchase preferences and history with clothing, food, housing, and physical addresses from various websites.[185] Transmitting users' personal information that does not contain identifying information and cannot be used to accurately track individuals to aggregator companies would not constitute a breach of layered information fiduciary duty.[186] By purchasing overall preference trend information of certain groups with common elements rather than buying recognizable data from aggregator companies, advertising companies would be able to provide relevant, preference-specific advertisements for users of a fixed group without infringing users' privacy.[187] It is worth noting that Facebook currently regards personal information with an IP address as unidentified data.[188] This practice harms data subjects' interests because IP addresses can easily be paired with each user's personally identifiable information.[189]

The third party may also be digital businesses that allow users to sign in with other digital corporations' accounts. If most software allows users to log in with their accounts on the largest platforms, large platforms will have a full range of users' personal information and preferences, and users' privacy will be compromised. Third parties also include other platforms' apps on online platforms, such as game apps on

183. *Id.* at 38 (articulating what circumstances and third-party behaviors will violate the proposed information fiduciary duty).

184. *Id.*

185. *See* Nizan Geslevich Packin, *Show Me the (Data About the) Money! What You Didn't Know About Data Aggregation Can Hurt You*, FORBES (Jan. 27, 2020, 10:04 PM), https://www.forbes.com/sites/nizangpackin/2020/01/27/show-me-the-data-about-the-money-what-you-didnt-know-about-data-aggregation-can-hurt-you/ [https://perma.cc/D429-5A55].

186. *See* Dobkin, *supra* note 30, at 41 ("Sharing aggregated data with third parties is consistent with an information fiduciary duty if no individual is personally identifiable and there are no unique identifiers for any one person.").

187. In fact, non-identifying information doesn't mean that a third party can't figure out the original owner of the information. When a substantial amount of personal information from various sources is aggregated, data without a name can be associated with the data subject to whom the information belongs, and the platform can deduce each digital consumer's preferences. *See* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/6EVY-RSPQ].

188. *See* Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/ [https://perma.cc/LBC6-HFLG].

189. *Id.*

Facebook.[190] If the platform's privacy agreement is inconsistent with that of the third-party app, DPOs must ensure platforms inform the user that the content of the two agreements is different. DPOs can be responsible for evaluating the specific content of the third-party privacy policy and ensuring that it complies with the provisions and the layered information fiduciary duty. There should be no difference between the layered information fiduciary duty of DPOs of third parties and DPOs of the big platform providers.[191]

Any breach of the above guidelines may constitute a breach of the layered information fiduciary duty. The burden of proof should be on DPOs to first prove that the layered information fiduciary duty owed to users has not been violated. The rationale for placing the burden of proof on the DPO is that DPOs have more information and a better understanding of the algorithms in the software used by the plaintiff, and the DPO may not actively provide evidence beneficial to users because the success of users may lead to the dismissal of the DPO by the company. The standard of care for violations of the information fiduciary duty should be ordinary negligence, a stricter standard than gross negligence, but damage awards should be capped. If there is no limit to damage awards, the risk of being a DPO will be extremely high, so it would be difficult to recruit high-quality talents willing to take the position.

2. Duty of Loyalty

Commentators and policymakers have proposed the introduction of the duty of loyalty to protect digital consumers' personal information.[192] When users trust the service provider to handle their personal information and disclose their information to them, the DPOs that advise service providers' data processing owe users a duty of loyalty. Violations of the duty of loyalty can focus on prohibitive provisions so that the company can identify the obvious red line.

The core of directors' duty of loyalty is that directors cannot have a conflict of interest and use their role to promote their own personal financial interests.[193] Specifically, directors should not obtain benefits for themselves or others, such as taking inappropriate business opportunities and self-dealing.[194] Therefore, the first specific duty under the layered information fiduciary duty's duty of loyalty is that

---

190. *See* Ian Bogost, *My Cow Game Extracted Your Facebook Data*, ATLANTIC (Mar. 22, 2018), https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/ [https://perma.cc/76BN-4Q6A].

191. *See* Balkin, *supra* note 180, at 2051–52.

192. *See*, *e.g.*, Richards & Hartzog, *supra* note 55, at 961; Data Care Act of 2021, S. 919, 117th Cong. (2021).

193. *See* Cede & Co. v. Technicolor, Inc., 634 A.2d 345, 361 (Del. 1993); Guth v. Loft, Inc., 5 A.2d 503, 510 (Del. 1939) ("[U]ndivided and unselfish loyalty to the corporation demands that there shall be no conflict between duty and self-interest.").

194. Beam ex rel. Martha Stewart Living Omnimedia, Inc. v. Stewart, 833 A.2d 961, 972, 975 (Del. Ch. 2003); *Cede & Co.*, 634 A.2d at 362 ("Classic examples of director self-interest in a business transaction involve either a director appearing on both sides of a transaction or a director receiving a personal benefit from a transaction not received by the shareholders generally.").

DPOs should ensure platforms do not gain benefits at the expense of users' personal information. DPOs' actions should be consistent with users' best interests.[195] The rationale is that most users lack expertise in novel technology and the consequences of the privacy agreement they signed;[196] their personal information is dominated by internet companies.

The following examples illustrate what happens when corporations with user information prioritize their own interests above those of the user. Instagram inculcates the concept that having an "ideal" body is important for girls, causing anxiety and suicidal ideation in teenagers.[197] Facebook also did not take effective measures to intervene in times when inflammatory words were used, resulting in an unstable environment that reduced people's sense of security and caused users to receive frightening information.[198] In these cases, technology companies put users' interests in a secondary position, not because they cannot address the issues threatening users' interests, but to maintain profit growth. A duty of loyalty would ensure companies are always alert so as to avoid conflicts of interest, deceptive data practices, and the protection of users' interests.

Directors are obligated not to abuse the company's statistical data, which the company cannot share with other companies, to avoid causing losses to the company.[199] Accordingly, DPOs should ensure that internet companies classify all the information collected and keep users' privacy information confidential without disclosing users' sensitive information. Companies may collect hundreds of pages of information for each customer without grading the information. For example, to accurately recommend high-matching partners to users, dating software companies first have users answer many detailed questions. The software may collect a wide range of over 800 pages of personal information from one user,[200] potentially

---

195. Other scholars also put forward similar proposals. *See, e.g.*, Richards & Hartzog, *supra* note 55, at 966–68, 992 (arguing that the difference between doctors and digital users is that patients and professionals can talk about patients' expectations directly. As long as doctors execute their agreed plan, they will attain the duty of loyalty. By contrast, it is difficult for platforms to directly obtain the privacy requirement from each user. At this time, the duty of loyalty requires the service provider to be responsible for users' best interests).

196. *See id.* at 968.

197. Dan Milmo & Clea Skopeliti, *Teenage Girls, Body Image and Instagram's 'Perfect Storm'*, GUARDIAN (Sept. 18, 2021), https://www.theguardian.com/technology/2021/sep/18/teenage-girls-body-image-and-instagrams-perfect-storm [https://perma.cc/XK2H-T7AY]; Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline [https://perma.cc/B798-VM3Z].

198. Newley Purnell & Jeff Horwitz, *Facebook Services Are Used to Spread Religious Hatred in India*, *Internal Documents Show*, WALL ST. J. (Oct. 23, 2021, 3:12 PM), https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354?mod=article_inline [https://perma.cc/3B96-4LCE].

199. *See* Beard Rsch., Inc. v. Kates, 8 A.3d 573, 602 (Del. Ch. 2010).

200. *See* Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, GUARDIAN (Sept. 26, 2017, 2:10 AM), https://www.

including many private questions such as gender preferences and religion. When the dating software shares this unclassified user information with other platforms, it transfers the information about what gender the user prefers along with more general data, such as the most-liked cuisine, to other corporations for the sake of its own interests.[201] This would constitute a violation of the duty of loyalty under the layered information fiduciary duty.

Under corporate law, directors cannot engage in unfair self-dealing with the corporation.[202] This means that the fiduciary duty does not accept deception and unfair behavior. This is reflected in privacy law in that any deceit of users constitutes a violation of the duty of loyalty. Specifically, the first rule should be for DPOs to ensure the platform acts in accordance with the privacy agreement. However, allowing enterprises to write agreements and obey the agreement they created will result in great differences in the implementation results between DPOs of various companies and generally loose privacy policies. First, enforcement would be more straightforward if, instead, a DPO association could create a standard agreement that can be modified only slightly by individual companies to tailor it to their situation.[203] Second, if an action ostensibly abides by the law but substantially violates the users' choice, it shall be deemed to violate the unfairness rule under this subsection. For example, the CCPA stipulates that users can freely choose whether platforms can sell their data.[204] In response, platforms began to exploit legal loopholes to share or exchange users' personal information with other companies without any monetary exchange.[205] This scenario would constitute a violation of the layered information fiduciary duty owed to users by the DPO. Third, DPOs should ensure that internet companies avoid manipulation. Users must have adequate autonomy,[206] such as rights to access, review, obtain, edit, correct, modify, opt out, dispose of, erase or revoke their own personal information collection, or purge their own browsing history upon request. DPOs need to ask digital platforms to provide a comprehensive procedure for users who would like to access or change their data and simplify internal approval procedures but retain the necessary process, such as reviewing whether the information belongs to the user themselves within a reasonable time limit after the user requests their data.

Under Delaware corporate law, directors are generally entitled to deference, under the business judgment rule, if they are unconflicted and/or their decisions are ratified

---

theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold [https://perma.cc/H6U3-7KMX].

201. *See* Natasha Singer & Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. TIMES, https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html [https://perma.cc/3559-YMUG] (Oct. 14, 2021).

202. *See* Sinclair Oil Corp. v. Levien, 280 A.2d 717, 720 (Del. 1971).

203. *See* Dobkin, *supra* note 30, at 44–45 (pointing out that privacy policies should be formulated in a user-friendly style instead of a long statement).

204. CAL. CIV. CODE § 1798.135 (2020).

205. *See* Bensinger, *supra* note 165.

206. *See* Citron & Solove, *supra* note 59, at 845–48 (finding that unlike many FTC unfair cases that are filed based on manipulation, few individual users sue for manipulation since many users are not aware of the occurrence of this behavior).

by a fully informed vote of the company's shareholders.[207] We should not adopt this approach for the layered information fiduciary duty because few users read or object to the generic privacy agreements that they click through and, therefore, they are not fully informed. DPOs should not be able to evade their layered information fiduciary duties through meaningless contracts of adhesion.[208] Moreover, it cannot be assumed in the privacy contract that users' consent to the current personal information use and disclosure implies blanket consent for future data use and disclosure.[209]

B. How Can the Layered Information Fiduciary Duty Be Applied to Multinational Corporations?

With the high integration of the world economy, the development of most multinational corporations is increasingly inseparable from cross-border data transmission. Consider the following example: the branches of the multinational corporations of country A located in country B transmit the user data of country B to the head offices in country A to analyze users' behaviors; multinational corporations belonging to country A share users' personal information collected by the branches located in country B with the branches of countries C and D to promote global operations. Without multinational legal constraints, the data recipient in another country in a multinational corporation may damage and abuse user information. Countries set many obstacles for data transmission between different countries to protect user data security.[210] Some countries such as Italy and Spain levy three percent digital services taxes on digital platforms,[211] while others implement data localization, requiring that sensitive information can only be saved on servers in their own country.[212] Additional taxes will increase a company's operating costs, and data

---

207. *See* DEL. CODE ANN. tit. 8, § 144 (2010); *see also* Kahn v. M & F Worldwide Corp., 88 A.3d 635, 645–46 (Del. 2014).

208. Commentators expressed similar views. *See, e.g.*, Richards & Hertzog, *supra* note 55, at 999 (arguing that companies cannot avoid the duty of loyalty because of users' assent to privacy agreements).

209. *See* GDPR, *supra* note 96, at art.7(2).

210. *See* Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J.L. & TECH. 182, 186 (2017).

211. *See* Dichiarazione Imposta sui servizi digitali (DST), AGENZIAENTRATE (June 23, 2022), https://www.agenziaentrate.gov.it/portale/web/guest/dichiarazione-imposta-sui-servizi-digitali/infogen-dichiarazione-imposta-sui-servizi-digitali-imprese [https://perma.cc/QU3M-GBMA]; del Impuesto sobre Determinados Servicios Digitales art. 11 (B.O.E. 2020, 4) (Spain) art. 11 (B.O.E. 2020, 4), https://www.boe.es/buscar/pdf/2020/BOE-A-2020-12355-consolidado.pdf [https://perma.cc/75SK-SJGY]. Most tax-collecting governments are European countries such as France, Turkey, and Hungary, with tax rates ranging from three percent to 7.5%. For details about tax rates, see Elke Asen & Daniel Bunn, *What European OECD Countries Are Doing About Digital Services Taxes*, TAX FOUND. (Nov. 22, 2021), https://taxfoundation.org/digital-tax-europe-2020/ [https://perma.cc/7T48-T9SJ].

212. For example, personal health records in Australia cannot be transmitted across borders. *See* Australian Digit. Health Agency, *Penalties for Misuse of Health Information*, MY HEALTH REC., https://www.myhealthrecord.gov.au/about/legislation-and-governance/penalties-for-misuse-health-information [https://perma.cc/7TDW-JDYJ] ("Holding, taking,

localization will affect global economic development.[213] The legal governance of the international transmission of information from many large global corporations has become an important problem to be solved.

For example, to deal with private data flows across national borders, the CCPA applies to any corporation that collects Californians' personal information, regardless of what country the business is physically located in.[214] The GDPR has jurisdiction over companies that have offices in the EU and non-EU institutions that provide digital businesses to end-users in the EU.[215] China's personal information protection law restricts companies that use personal data in China and overseas tech platforms that use the personal data of Chinese digital consumers.[216] *The New York Times* states that overseas users' data will be gathered in users' home states and transmitted to the main U.S. office or subsidiaries and partners located in other countries.[217] The GDPR allows personal information to be transmitted to non-EU countries as long as the receiving side sufficiently protects personal information.[218] It is still unclear if these new laws will succeed in preventing the international transmission of sensitive personal data.

When companies face these different regulatory rules from various countries, they have three options: (1) adopt a global privacy policy according to the country with the strictest protection measures, [219] (2) adopt a different privacy agreement in each individual country the company operates in, or (3) withdraw from the country to

---

processing or handling, records held for the purposes of the My Health Record system outside Australia, or causing someone else to do so . . . [will result in a] [c]ivil penalty of up to 1,500 penalty units (up to 7,500 penalty units for bodies corporate); [c]riminal penalty of up to five years imprisonment and/or 300 penalty units (up to 1,500 penalty units for bodies corporate)[.]"); *see also* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 683–704 (2015) (discussing the data localization in thirteen countries such as Nigeria (prohibited to export government related data) and South Korea (regulating data related to maps)).

213. *See* Gary Beach, *GDPR Is Almost Here, Let the Data Protection Officer Talent Race Begin*, WALL ST. J. (Mar. 1, 2018, 11:03 AM), https://www.wsj.com/articles/gdpr-is-almost-here-let-the-data-protection-officer-talent-race-begin-1519920221 [https://perma.cc/FZ8N-HS8X] (illustrating that GDPR has created "barriers to globalization" leading many companies to withdraw or not enter the market in specific areas, thus further affecting the world economy).

214. CAL. CIV. CODE § 1798.140(c)(1).

215. GDPR, *supra* note 96, at art. 3(1), (2).

216. Personal Information Protection Law of the People's Republic of China [PIPL] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021) art. 3, P.R.C. LAWS, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm [https://perma.cc/AT7J-LNVF].

217. *The New York Times Company Privacy Policy*, N.Y. TIMES, https://www.nytimes.com/privacy/privacy-policy#how-is-my-information-transferred-internationally [https://perma.cc/SW6L-DXJA] (Aug. 10, 2022).

218. GDPR, *supra* note 96, at art. 45(1).

219. *See* Olivia Solon, *How Europe's 'Breakthrough' Privacy Law Takes on Facebook and Google*, GUARDIAN (Apr. 19, 2018, 3:01 AM), https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation [https://perma.cc/4AAN-UNPV].

avoid compliance costs. In the long run, variance in the strictness of countries' privacy laws hinders industrial innovation and affects economic development.

Effective management of data flow across borders should be the key. However, there are only scattered agreements between select countries, such as the Trans-Atlantic Data Privacy Framework.[220] The scattered agreements lead to loopholes in cross-border data transmission. Ideally, the field of international data flow would adopt a unified, familiar, easily accepted fiduciary concept. Thus, all multinational corporations should adopt the layered information fiduciary duty.

The information fiduciary duty of DPOs of multinational corporations is roughly the same as the duty of care and loyalty detailed above. For example, under the duty of care, the DPO needs to ensure that users are informed of which part of the data will go to which countries, why the data needs to be transmitted to foreign countries, and the risks involved with transmitting the data. Some users may refuse to consent to the transmission of their data after they understand the details. The layered information fiduciary duty can reduce potential privacy disclosure by asking multinational corporations' DPOs in various countries to limit the transnational transmission of data to as little data as possible. The duty of care under layered information fiduciary duty requires DPOs to evaluate third country branches' vulnerabilities and security, which will help to reduce the risk of damage to users' personal information at the beginning. DPOs can ensure that encryption technology or pseudonymization is used in cross-border data transmission to ensure data security.

Each branch within a multinational corporation can have its own independent, professional DPO or a team led by a DPO that can handle the user privacy issues related to each branch. In case of data leakage and other violations of users' privacy after data transmission, the DPO of the breached company shall inform and notify all affected entities and data processing departments of the potential damages resulting from the leak as well as the prepared response plan. DPOs of multinational companies in the same data supply chain can organize an alliance to regularly discuss the performance of their layered information fiduciary duty in the cross-border flow of data and how to reduce users' risk and record their best and worst practices to be disclosed to the public. That way, enterprises that repeatedly violate the best practices can be identified by users. The International Association of Privacy Professionals (IAPP) should also include the layered information fiduciary duty in the training and tests of the Certified Information Privacy Professionals (CIPP).[221]

In the process of information transmission, how can the layered information fiduciary duty minimize the risk of cross-border transmission of user information? In the modern world, many countries, including the United States, United Kingdom,

---

220. Press Release, White House, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ [https://perma.cc/7ELG-DEUU]; RACHEL F. FEFER & KRISTIN ARCHICK, U.S.-EU TRANS-ATLANTIC DATA PRIVACY FRAMEWORK, IF11613 (2022), https://crsreports.congress.gov/product/pdf/IF/IF11613 [https://perma.cc/DV2T-NTXC].

221. CIPP Certification, IAPP, https://iapp.org/certify/cipp/ [https://perma.cc/LX4C-7ZCP].

Germany, Japan, and China, have corporate laws imposing fiduciary duties on directors and executives. Similar concepts in these countries cause multinational corporations' governance to have relatively unified norms. This is helpful for directors and executives to understand their duties and what they may be punished for if they fail to fulfill their roles or effectively perform their duties. Some Asian countries, such as China, have also formulated privacy laws,[222] demonstrating that strengthening the governance of privacy is a global trend. Imposing information fiduciary duties on U.S. companies will encourage countries around the world to establish similar concepts while formulating privacy laws, greatly strengthening the supervision of privacy issues of multinational corporations. In this way, when a company's information is transmitted to another country, it would be difficult for the company to exploit legal loopholes through cross-border transmission because the receiver corporation would have also adopted similar information fiduciary duties. The information fiduciary duty can be used as a method for countries around the world to achieve a more unified data governance model. This will be conducive to cross-border law enforcement cooperation among countries. Compared with the general internal rules, the advantage of the layered information fiduciary duty is that it can be applied not only in the subsidiaries of multinational corporations but also in the transferring of users' data between multinational corporations. When all multinational companies have a uniform information fiduciary duty, they will gradually establish a better practice of good data management. Ideally, when a company wrongfully obtains data, the DPO will arrange for engineers to actively destroy it.[223]

It may not be easy for multinational corporations to directly and widely adopt the layered information fiduciary duty. It may be helpful to use the existing user privacy protection platform of international organizations to help promote the implementation of information fiduciary obligations. Relevant international organizations have already created basic frameworks for cross-border information sharing. For example, the Organization for Economic Co-operation and Development (OECD) promotes a scheme called the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[224] Countries that are party to these agreements are a perfect place to pilot the layered information fiduciary duty. The GDPR can regard the countries with the layered information fiduciary duty as important in the effort to protect user privacy, as part of evaluating the sufficiency of Article 45's "adequate level of protection."[225] The adoption of the layered information fiduciary duty means that countries are adopting stricter user-privacy protection standards. Countries willing to implement the layered information

---

222. The Chinese Personal Information Protection Law was passed on August 20, 2021. Josh Horwitz, *China Passes New Personal Data Privacy Law, to Take Effect Nov. 1*, REUTERS (Aug. 20, 2021, 1:46 AM), https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/ [https://perma.cc/T2JU-BHTY].

223. DOUWE KORFF & MARIE GEORGES, THE DPO HANDBOOK 144 (2019), https://ssrn.com/abstract=3428957 [https://perma.cc/Y65P-7WXA].

224. *OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/3V8K-PQ74].

225. GDPR, *supra* note 96, art. 45(1).

fiduciary duty can send preferential taxation to each other or simplify the declaration process of data transmission.[226] The consequences of breaching the layered information fiduciary duty of each country may differ. However, the general concept, direction, and specific duties required will be basically the same in each country, ensuring it can be implemented across borders. The concept of a similar layered information fiduciary duty between countries also has the advantage of avoiding the potential conflict of privacy protection laws in various countries, reducing the likelihood that users are shirked by countries with differing laws. The sender and the receiver bear the same layered information fiduciary duty, but the sender as the initiator should account for a larger proportion of the specific amount of compensation. If the layered information fiduciary duty proves to be practical and useful, it should not be difficult to adapt around the world because many countries are very familiar with traditional fiduciary duties, which have been developed and implemented routinely for decades. Over time, some companies may reduce risks by not transmitting information to multinational companies that do not have layered information fiduciary duty, encouraging more companies to embrace the layered information fiduciary duty to expand their business. Countries can also sign additional treaties on information fiduciary duties to promote consensus and supervision of the cross-border flow of information. In addition, most corporations share digital consumers' data with their subsidiaries that comply with similar privacy policies. By requiring the subsidiary's privacy policy to comply with the layered information fiduciary duty of the country where the parent company's headquarters is located, the data branches of the multinational company in other countries can be managed without directly regulating the subsidiary located in another jurisdiction.[227] This can make the laws of the countries where the branches and head offices are located consistent. If the law of the country where the branch of a multinational corporation is located is more stringent than the requirements of the information fiduciary duty, the law of the country where the branch is located shall prevail.

III. IMPLICATIONS

A. What Can Corporate Law Do to Solve the Problem of Tech Companies' Invasion of End-Users' Personal Privacy?

The layered information fiduciary duty is closely related to corporate governance because DPOs that violate the layered information fiduciary duty will face potential liability for compensation. DPOs should thus fulfill the layered information fiduciary duty in the decision-making process. The layered information fiduciary duty should be added to the Model Business Corporation Act (MBCA)[228] and the Delaware

226. Balkin, *supra* note 1, at 1229.

227. Balkin, *supra* note 180, at 2031.

228. The MBCA, which was issued by the American Bar Association, has been adopted by around thirty states and has a wide impact on the field of corporate law. For a fuller explanation of the MBCA, see *2016 Revision to Model Business Corporation Act Makes Its Debut*, ABA (Dec. 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/12/10_mbca [https://perma.cc/QBX5-KTT4].

General Corporation Law (DGCL),[229] helping various parties fully understand their roles.

The GDPR stipulates that corporations hire DPOs to supervise the use of data.[230] Many companies might also employ a Chief Compliance Officer (CCO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), and virtual Chief Information Security Officer (vCISO). In order to implement the layered information fiduciary duty, Delaware corporate law should require management and directors to hire DPOs to advise and monitor how their corporation uses users' personal information and generate annual reports that users can access. DPOs should report to the CEO every quarter on the implementation of the layered information fiduciary duty and execute specific measures and suggestions for improving the implementation of the layered information fiduciary duty for the next quarter. The DPO should not only oversee whether the company has fulfilled its duty of care and loyalty to users but also add engineers' efforts to protect users' privacy and how companies investigate and respond to users' privacy-related complaints to the quarterly performance appraisal.[231] DPOs would have independent decision-making ability and could guide the privacy commissioner on how to solve users' dissatisfaction. DPOs would have the obligation to fulfill the layered information fiduciary duty and ensure engineers' design is consistent with the layered information fiduciary duty's content. DPOs who would take the layered information fiduciary duty could be changed regularly every five years. DPOs would balance the interests of shareholders and the company and serve as the corporation's intermediary for the benefit of the company, that is, the common welfare services of all people closely related to the enterprise, such as the local community and creditors.[232] DPOs would be partially personally liable for the company's losses caused by privacy issues,[233] so as to incentivize them to fulfill their fiduciary duties more diligently.

B. Remedies

The remedies available under the privacy law should punish DPOs that violate users' privacy rights, remedy users' losses, and deter other companies that may be

---

229. Around half of the influential large corporations are registered in Delaware, so Delaware's corporate law affects the formulation of corporate law in the other states and even has influence globally. *See Why Businesses Choose Delaware*, DELAWARE.GOV, https://corplaw.delaware.gov/why-businesses-choose-delaware/ [https://perma.cc/F7WJ-CD4E].

230. GDPR, *supra* note 96, at art. 37.

231. *See, e.g.*, Waldman, *supra* note 19, at 833 ("A more powerful approach would be to evaluate subordinates for their substantive privacy progress—namely, whether a new product collects the least amount of data necessary, limits data collection for a single purpose, includes designs that make it easy for users to exercise their rights, eliminates dark patterns, protects the unique privacy needs of marginalized populations, and so forth.").

232. *Id.* at 783.

233. *Id.* at 833 ("[E]levating the CPO to a board-level position would help get the message across . . . . Business unit leaders should not just have local responsibility for integrating privacy into their work; they should also be held responsible for substantive results.").

inclined to violate the privacy law. DPOs would enter an indemnity agreement as part of their employment contract. DPOs could request the company to indemnify them, and the company could choose not to indemnify intentional breaches of fiduciary duties. The availability of damages incentivizes people to vindicate their rights.[234] Although a variety of remedies already exist in privacy infringement cases, courts' high standard for proving damages, such as whether the infringement has brought about genuine financial or reputation damage, leaves the privacy rights of the majority of plaintiffs unprotected.[235]

Privacy scholars, such as Citron and Solove, propose that courts may ask plaintiffs to provide proof of damage when plaintiffs desire indemnification of their losses rather than injunctive relief.[236] Privacy lawsuits will attract public and media attention and might affect the company's reputation, which may cause the internet giant to lose some users and cause economic losses that may be no less than the amount of compensation in the lawsuit. In addition, it should be noted that arbitration should not be one of the options for users and DPOs to resolve disputes because arbitrations are generally conducted privately. Allowing arbitrations would undermine the effectiveness of the layered information fiduciary duty because companies and DPOs would not suffer the reputational damage necessary to deter privacy breaches.

In the initial implementation stage, several large companies could be used as test sites for at least six months. For companies that enforce the layered information fiduciary duty at the beginning, the law enforcement department could temporarily and partially exempt various complex requirements.[237] For the GDPR, regulators can penalize corporations that violate privacy rules for no more than four percent of their global income.[238] Such a high penalty is set because a small penalty is not enough to attract large corporations' attention to data protection.[239] The punishment for violating the layered information fiduciary duty can be based on this compensation standard, because most companies might have accepted the amount of four percent after the implementation of the GDPR for four years.

CONCLUSION

In today's world, companies routinely violate users' privacy, necessitating new legal weapons to protect digital consumers. Establishing a double-track and nonoverlapping layered information fiduciary duty is a feasible path to protect users' privacy in this information age. Adding the layered information fiduciary duty can improve the confusing legal patchwork and the theoretical disputes caused by the information fiduciary duty. A layered information fiduciary duty will help establish

---

234. Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1343 (2019).

235. Citron & Solove, *supra* note 59, at 801–02, 850.

236. *Id.* at 823.

237. Zittrain, *supra* note 111 (arguing that the information fiduciary can be freely chosen by both parties like the financial services institutions' fiduciary duty. Many clients would prefer an adviser over a broker because the adviser would be the client's fiduciary.).

238. GDPR, *supra* note 96, at art. 83(5).

239. Jones & Kaminski, *supra* note 78, at 106.

a uniform system to save privacy from dying, will prevent corporations from trampling on users' trust, and will enable users to better understand the details of their privacy rights. The DPOs under the layered information fiduciary duty focus not only on actively protecting users' personal information but also on preventing engineers and other involved parties from doing things that can harm users. The ideal outcome of privacy law regulation is that users become the masters of their own information in a real sense. Without the layered information fiduciary duty, the risk of personal information being exposed will increase and the protection of personal information will not be guaranteed. This Article defines why the information fiduciary duty is needed and the specific connotation and composition of the layered information fiduciary duty, including the duty of care and duty of loyalty, how to implement it in multinational corporations, and why the application of the layered information fiduciary duty in multinational corporations will play a practical role in protecting users' information so as to build a comprehensive framework for information fiduciary duty.