Fordham Law Review

Volume 90 | Issue 4 Article 2

2022

Serious Notice: A Celebration, Discussion, and Recognition of Joel Reidenberg's Work on Privacy Notices and Disclosures

Tal Z. Zarsky
University of Haifa

SERIOUS NOTICE: A CELEBRATION, DISCUSSION, AND RECOGNITION OF JOEL REIDENBERG'S WORK ON PRIVACY NOTICES AND DISCLOSURES

*Tal Z. Zarsky**

This Essay pays tribute to Professor Joel Reidenberg's rich academic career and, specifically, to his contributions to the study of privacy policies. In doing so, this Essay takes a close look at privacy policies and possible ways to effectively intermediate their content through various labeling schemes. While severely flawed, privacy policies are here to stay. Therefore, an in-depth analysis of ways to enhance their efficiency is merited. This Essay thus examines key strategies for privacy-related intermediation, obstacles, and problems arising in the process, as well as possible solutions. The analysis weaves together theoretical and empirical privacy law scholarship (much of it by Professor Reidenberg), "classic" work on the limits of disclosure policy, and general scholarship on certification.

Part I of this Essay provides a brief introduction to privacy policies and the challenges of their intermediation. Part II examines the additional steps that must be taken to ensure that privacy intermediation is effective and efficient in terms of the system's design, especially through setting disclosure objectives and priorities. It also addresses the use of personalized disclosure and its possible shortcomings. Part III assumes that privacy intermediation is successful and confronts the potential problems that may lead to the trivialization of labels and rankings over time. These dynamics result from a possible flood of appeals for reevaluation and ensuing grade inflation. This part also briefly explains how such concerns may be mitigated through proper design, tailored disclosures, and tinkering with the liability regime of intermediaries. This Essay concludes with some parting thoughts about Reidenberg's substantial contribution to "law and technology" scholarship and the ways others may develop it in years to come.

---

* Vice Dean and Professor of Law, University of Haifa, Faculty of Law. This Essay was prepared in connection with a symposium to celebrate the scholarly and personal contributions of Joel Reidenberg. The event was cancelled in light of the COVID-19 pandemic. This Essay was written during my visit to the University of Pennsylvania Carey School of Law as an Israel Institute Faculty Fellow. It also benefited from partial funding from the Haifa Center for Cyber Law and Policy (CCLP). I thank Shmuel Becher, Ayelet Sela, and Mark Verstraete, as well as the participants of the Law and Technology Workshop at Bar-Ilan University for their helpful comments and Shani Leibovitch for her excellent assistance in research.

INTRODUCTION: MOTIVATION AND PERSONAL PRELUDE

This Essay takes a close look at privacy policies. The motivation for this somewhat mundane inquiry is simple: privacy policies are here to stay. Therefore, we must figure out how to live with and utilize them. Although they are deeply flawed, there are some ways in which the disclosure process they enable could be improved. One way may be through intermediation, which can help convey the message of these policies to the public at large. This Essay examines key strategies of privacy-related intermediation, mostly by relying on labels. It addresses the obstacles and problems related to the main challenges of privacy policy labeling and suggests possible solutions that utilize both human and automated processes. It also addresses secondary challenges, such as problematic feedback loops between firms and labeling intermediaries, that may ensue if labeling schemes prove popular and effective. The analysis that follows weaves together theoretical and empirical privacy law scholarship, "classic" work on the limits of disclosure policy, and general scholarship on certification. This Essay also offers concrete policy recommendations regarding the proper process of structuring labels, noting the importance of formulating objectives and priorities early on.

The initial motivational paragraph for this Essay conveys only a half-truth. Although privacy policies are highly relevant and important in the privacy and tech-law realm, the motivation for this exploration is mostly personal. I

wish to pay tribute to the important work of Professor Joel Reidenberg by linking together and discussing several papers he published in recent years on topics related to privacy disclosures and labels. These papers added crucial knowledge and depth to a key piece of the overall information privacy law puzzle.

In the last two decades, I have spent many hours with Joel Reidenberg not only by reading his work but also in personal encounters. Initially, it was Joel's innovative scholarship that introduced me to a broad array of key legal concepts from the realm of law and technology. But many physical meetings followed. I had the privilege and pleasure of engaging with Joel in multiple locations over three continents. We often talked about culture, religion, history, and family. Yet, naturally, most of our conversations were about privacy law and technology.

Every time our conversations shifted to the discussion of privacy-related issues, my ongoing impression of Joel Reidenberg was that he always took these matters very seriously. Joel's passion for privacy issues was apparent from the first time I encountered his work over twenty years ago. I remember clearly that, at our first face-to-face meeting a long time ago, Joel enthusiastically told me, a total stranger at the time, of a recent and somewhat obscure privacy-related legal development. After our conversation, as I walked away, I noted to myself that I should strive to be more like Joel; I should be taking things more seriously and convey that sense to others. I continue striving to do so, with limited success. Although he is now gone, Joel continues to inspire me and many others of my generation, still setting an unachievable standard.

Joel Reidenberg applied his rigor and enthusiasm to an abundance of privacy-related topics. He was a frequent virtual guest in my classroom. Early on, he educated me and others on international personal data flows, government surveillance, and educational privacy. There is much to discuss about every one of these key contributions, as well as many others, and some of my esteemed colleagues addressed them in recent academic scholarship.[1] Yet, in this Essay, I choose to focus on a relatively recent thread in Joel's scholarship—perhaps his last writings—on the nature of privacy disclosures. This work, which Joel carried out with several coauthors, has contributed constructive insights to promote the use of privacy disclosures. To achieve these insights, which cautiously advocate the use of privacy-related public disclosures, Joel Reidenberg set aside existing overall skepticism toward such disclosure practices and reconsidered how and when they should be applied.[2] It is, in other words, serious work by a serious scholar in an area in which many others have contributed mostly mockery and criticism.

---

1. *See 25th Annual BTLJ-BCLT Symposium: Lex Informatica: The Formulation of Information Policy Rules Through Technology*, BERKLEY L., https://www.law.berkeley.edu/research/bclt/bcltevents/btlj-bclt-symposium-lex-informatica-the-formulation-of-information-policy-rules-through-technology/ [https://perma.cc/M93S-JN6N] (last visited Feb. 2, 2022).

2. Professor Ari Waldman noted: "There is voluminous scholarship on privacy notices and their faults. Less work has been done on their design." Ari Ezra Waldman, *Privacy,*

Joel Reidenberg built bridges and brought worlds together—something he excelled in both personally and professionally. In other scholarship, he brought U.S. and European law closer together, generating insights about German and French law for the American audience.[3] He also integrated the historical lex mercatoria rules into the digital age.[4] In the topic I discuss here, Reidenberg brought together the issue of privacy and the broader scholarship devoted to examining, critiquing, and designing disclosure strategies.[5]

This Essay takes a close look at disclosure policies with reference to privacy, continually turning and returning to Reidenberg's work as a point of reference and inspiration. It focuses on the importance of, feasibility of, and ability to optimize intermediation of such disclosure to the broader public, especially through labeling—all given the understanding that privacy policies will most likely continue to dominate the discourse regarding privacy-related disclosures. Labels are structured forms of disclosure with unique characteristics and established design and content. The objective of a label is to convey a limited, but important, set of facts and statements to users, in a manner they can grasp quickly and effectively. The intricacies of labeling are widely discussed in a range of contexts. Below, I provide a cursory glimpse into how these might relate to the privacy disclosure discourse.[6]

Part I of this Essay begins with a brief introduction to privacy policies and the challenges of intermediation. Next, it introduces Reidenberg's recent seminal contributions to the discussion of privacy notification and the ways that intermediation of such information may be carried out, focusing on the use of labels. It does so by providing limited commentary and framing Reidenberg's work within several broader themes related to the study of privacy policies.

Part II examines the additional steps that must be taken to ensure that privacy intermediation is effective and efficient in terms of the system's design. Based on foundational insights derived from the broader discourse on regulatory disclosure, Part II points out the importance of setting disclosure objectives and priorities. It further explains how this may be achieved in the area of privacy, relying on methodologies Reidenberg and others developed. The discussion also addresses the use of personalized disclosure and its possible shortcomings.

Part III assumes that privacy intermediation is successful and confronts potential problems that could lead to the trivialization of labels and rankings over time. These relate to a possible flood of appeals for reevaluation and

---

Notice, and Design, 21 STAN. TECH. L. REV. 74, 81 (2018). For a discussion of both forms of scholarship, see M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1054–55 (2012).

3. *See, e.g.*, Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS 261 (2002).

4. *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

5. For a discussion of this void, see Waldman, *supra* note 2, at 77.

6. *See infra* notes 91–95.

ensuing "grade inflation." Such concerns are likely to compromise the labeling process—a risk somewhat ironically rendered more acute as the means of intermediation, such as labels or ranking, gain importance and salience. This part also briefly explains how these concerns, which must be addressed early on to ensure effective intermediation, may be mitigated through proper design, disclosures, and tinkering with the liability regime of the intermediaries. The Essay concludes with some parting thoughts about Reidenberg's substantial contribution to this area of scholarship and how it may be developed by others in years to come.

I. REIDENBERG (AND OTHERS) ON ASSESSING AND IMPROVING PRIVACY DISCLOSURES: MAKING INTERMEDIATION WORK

This part closely examines how information included in privacy policies can be effectively conveyed to the public, while framing, presenting, and commenting on Reidenberg's work on this issue. It begins by noting the substantial flaws in the common forms of privacy disclosures, given the difficulty of understanding the diverse, immense, and dense texts. Next, it considers whether the vastness of the task may be overcome by using innovative intermediation techniques. After a brief primer on the nature of privacy-related intermediation and its design options, this part examines the utility of applying crowdsourcing and AI-driven measures to streamline intermediation and relying, partially, on pre-approved texts. The analysis addresses the shortcomings of such methods and the ways their proper integration may overcome these challenges.

A. Privacy Policies: Neither Privacy nor a Policy

It is fair to assume that every entity interacting digitally with the public while collecting personal information offers some form of a "privacy policy," a public-facing document detailing how the firm collects, analyzes, and uses personal data. The motivations for drafting and presenting this document may be legal, promotional, and at times, even genuinely part of an attempt to educate the public about the firm's use of personal information.[7] Nevertheless, the document is very often filled with cryptic jargon,[8] hidden from the eye and accessible only through a link tucked away at the bottom of a webpage.

The concept of the "privacy policy" displays impressive and surprising resilience. After all, few ideas have been belabored more than privacy

7. *Cf.* David Hoffman, *Relational Contracts of Adhesion*, 85 U. CHI. L. REV. 1395, 1399 (2018) (arguing terms can serve a precatory role, encouraging specific user behavior on the platform).

8. For a recent study indicating that privacy policies are (still) unreadable for the average user even after the enactment of the GDPR, see Shmuel I. Becher & Uri Benoliel, *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*, *in* CONSUMER LAW AND ECONOMICS 179 (Klaus Mathis & Avishalom Tor eds., 2020).

disclosures and "policies."[9] Yet, the privacy policy seems to survive and thrive, at least as a point of reference in practical and academic discussions of privacy law and policy.[10] As Reidenberg noted, privacy policies remain the "single most important source of information for users to attempt to learn how companies collect, use, and share [personal] data."[11] One might speculate that the miraculous resilience of privacy policies is quite likely the result of the fact that they are the *only* privacy-enhancing measure almost everyone can agree on implementing. In other words, they are the lowest common denominator in the privacy regulation realm. For some, they are an initial steppingstone toward additional, more aggressive privacy-enhancing regulatory measures. For others, privacy policies are the least intrusive (and innovation-impeding) measure that privacy regulation might mandate to inform users and bridge information asymmetries.[12]

At the same time, privacy policies are clearly and utterly flawed. As Professor Joseph Turow insightfully noted, the policies should not even be allowed to carry a manipulative title. The term "privacy policy" suggests that the disclosing entity provides a minimal, if not reasonable, level of privacy protection, which it often does not.[13] In view of this problematic reality, scholars have naturally tended to discuss and criticize privacy policies. They noted early on how the notion that users meaningfully consent to the practices detailed in the privacy policy is nothing short of a bad joke because of the information asymmetry and systematic user myopia.[14] Indeed, no one reads privacy policies anyway.[15] Life is too short to be spent

---

9. Joel R. Reidenberg et al., *Trustworthy Privacy Indicators: Grades, Labels, Certifications and Dashboards*, 96 WASH. U. L. REV. 1409, 1412 (2019).

10. For example, see the discussion of mandating privacy notices as part of the White House's Consumer Privacy Bill of Rights. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 14 (2012) [hereinafter "White House Report"], https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/FKS9-GJ9X].

11. Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 39 (2015).

12. For a similar and more detailed framing of privacy policies, see Calo, *supra* note 2, at 1029, 1048. For an argument that disclosure policies generally do not provide an adequate compromise between the competing forces of nonintervention and calls for aggressive and, at times, intrusive regulation, see generally Doron Teichman, *Too Little, Too Much, Not Just Right: Seduction by Contract and the Desirable Scope of Contract Regulation*, 9 JERUSALEM REV. LEGAL STUD. 52 (2014).

13. JOSEPH TUROW, ANNENBERG PUB. POL'Y CTR. OF THE UNIV. OF PA., AMERICANS ONLINE PRIVACY: THE SYSTEM IS BROKEN 3 (2003) ("57% of U.S. adults who use the internet at home believe incorrectly that when a website has a privacy policy, it will not share their personal information with other websites or companies."). Although this study dates back to 2003, it may be wishful thinking to believe things have changed by 2022.

14. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1265 (1998). For additional sources, see Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y INFO. SOC'Y 485, 491, 494 (2015).

15. Lior Jacob Strahilevitz & Matthew B. Kugler**,** *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S71 (2016); *see also* OMRI BEN-SHAHAR & CARL E.

pondering and contemplating the nonnegotiable, complicated, and long legal terms of the privacy policies.[16]

Over the years, criticism of the ineffectiveness and consequent insignificance of privacy notices has become increasingly pervasive and persuasive, given several technological and social changes. The notices have become longer,[17] and with the growing use of smartphones, the screens on which to view them have shrunk.[18] At times, there is no screen on which to review the privacy policies at all. When using gadgets and other technologies within the "Internet of Things" (toys, bracelets, wearables, etc.), there is merely a link or reference to a relevant text pertaining to the privacy policy.[19] Many of these applications constantly collect personal data,[20] merely providing some notice regarding their privacy policies on a product-related webpage.[21]

Furthermore, the privacy policy discussion has morphed into an extension of a broader one, having to do with the troubles of disclosures in general. Evidence has shown that, in this extended context, disclosure policies are often unable to achieve their objectives of educating the public and enabling meaningful choice.[22] Discussions about privacy policies have blended into the broader discourse regarding fairness of the legal fiction that foundational documents, such as consumer form contracts, are part of the constructive knowledge of users. Users rarely read and comprehend these documents;[23] yet, according to accepted doctrine, the content binds the relevant contractual parties. In other words, the application of an overarching duty to read renders

---

SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 67–68 (2014).

16. On the length of time reading such notices requires, see Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 543 (2008).

17. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 148; Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/9ZD2-FYMB].

18. White House Report, *supra* note 10, at 15.

19. Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 90, 95 (2014) (noting the limited way privacy policies were presented to consumers of Internet of Things (IoT) devices). To address this concern, scholars have suggested adding labels to IoT devices. *See* ALEXANDR RAILEAN & DELPHINE REINHARDT, LET THERE BE LITE: DESIGN AND EVALUATION OF A LABEL FOR IOT TRANSPARENCY ENHANCEMENT (2018).

20. ELLEN P. GOODMAN, ASPEN INST., THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS 23 (2015).

21. Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399, 419 (2019) (demonstrating how, in the case of toys, privacy policies are displayed on links available elsewhere); *see also* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 59 (2019) (discussing the weakening of notice in the area of wearables and the "sensing net").

22. BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 3 ("'Mandated disclosure' may be the most common and least successful regulatory technique in American law.").

23. *See* Yanees Bakos et al., *Does Anyone Read the Fine Print?: Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014).

even nonreading parties subject to certain rules and requirements, including those related to privacy.[24]

B. Reidenberg and Privacy Policy Intermediation: Key Contributions

In several influential analytical and empirical papers, Reidenberg and his coauthors sought to promote proper privacy disclosures. As a starting point, they chose modest objectives for personal data usage disclosures, framing them as part of the need to "provide consumers with more meaningful notice, empower consumers, and nudge data processors to improve their privacy notices and practices."[25] Much can be said about each of these elements. In the interest of brevity, however, in this Essay, I accept the first two objectives—notice and empowerment—as sufficiently sound, without further analysis. Therefore, they will serve as the point of reference for the rest of this discussion. Providing robust notice and empowering users can also easily be premised on several theories, including enhancing user autonomy and, possibly, the dynamics that promote privacy through market pressures. I set the "nudging" element aside because it creates substantial complications and invites nontrivial criticism of the legitimacy of "nudging" efforts and their questionable success.[26]

Professor Reidenberg and his team moved forward to address possible disclosures. The underlying assumption of the overall project was that individuals do not (and possibly cannot) independently review and sufficiently comprehend entire privacy policies in their current full format; some form of effective intermediation must unfold.[27] Thus, the question for Reidenberg and his team was how such intermediation is best achieved.

1. Primer on Privacy Policy Intermediation

There are almost endless formats and models for privacy intermediation.[28] An extensive literature describes efforts to enable effective intermediation using technology and management-based tools.[29] Yet, to date, the success of such intermediation is limited for a variety of reasons. Here, I set aside backward-looking discussions of historical failures to join in on Reidenberg's contemporary analysis, given recent technological

24. *See* Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C. L. REV. 2255, 2260–64 (2019) (discussing the justifications and ramifications of the duty to read consumer contracts).

25. Reidenberg et al., *supra* note 9, at 1414.

26. For a discussion of the critiques of nudging and possible responses, see Calo, *supra* note 2, at 767–77.

27. *See generally* Reidenberg et al., *supra* note 9.

28. Irene Kamara & Paul De Hert, *Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape*, *in* PRIVACY AND DATA PROTECTION SEALS 12, 70–78 (Rowena Rodrigues & Vagelis Papakonstantinou eds., 2018).

29. *See, e.g.*, PATRICK GAGE KELLEY ET AL., A "NUTRITION LABEL" FOR PRIVACY (2009). For a recent discussion, see Christof Koolen, *Transparency and Consent in Data-Driven Smart Environments*, 7 EUR. DATA PROT. L. REV. 174 (2021).

developments that may prove to be game changers that finally enable effective privacy-related disclosure.[30]

Before doing so, consider a short primer on the nuts and bolts of privacy policy intermediation, specifically regarding who must carry it out and what it should include. Intermediation involves both simplifying and vetting privacy disclosures. On the face of it, at least the simplification task could be carried out by the firms themselves by providing an easily identifiable icon or other quick indicators of the privacy setting.[31] Furthermore, the firm can publish both a long (and exhaustive) and a short (and intuitive) version of its policies.[32] This would be a form of self-reporting, possibly featuring adherence to predefined grades, certificates, or labels for the abbreviated self-reporting, which may be audited ex post.[33]

This option of self-regulation or reporting, however, is quite likely doomed to fail given firms' temptation to inaccurately summarize and categorize their privacy practices.[34] Using the terminology developed in the regulation scholarship concerning certification, such self-reported information might lack both "input" and "output" legitimacy.[35] Input legitimacy relates to "inclusiveness and transparency of the internal decision-making process with regard to setting standards" as to what is included in the limited and condensed disclosure.[36] This process might be compromised when a firm frames its own condensed text. For example, in the case of a label, a firm may choose to highlight its strengths and hide (or even refrain from mentioning) its weaknesses within the limited space of the label. This concern is already apparent in environmental matters, where a tension has developed between eco-labels and "greenwashing," the practice of providing

30. *See* Reidenberg et al., *supra* note 9, at 1429, 1460 (discussing various failed intermediation attempts such as problems with Mozilla's icon scheme and the ToS;DR project).

31. *See* HANA HABIB ET AL., TOGGLES, DOLLAR SIGNS, AND TRIANGLES: HOW TO (IN)EFFECTIVELY CONVEY PRIVACY CHOICES WITH ICONS AND LINK TEXTS §§ 3–7 (2021), https://dl.acm.org/doi/pdf/10.1145/3411764.3445387 [https://perma.cc/NT5V-8EK4] (discussing the existing scholarship and experience with privacy icons, as well as a test as to the effectiveness of various forms of privacy icons).

32. Note that the conventional "long" privacy policy is a form of intermediation, as well, because it conveys in relatively simple language what the scripts and the source codes of the website and apps are carrying out.

33. To some extent, this is the "layered disclosure" scheme advocated by some EU regulators. *See* EUR. DATA PROT. BD., GUIDELINES 3/2019 ON THE PROCESSING OF PERSONAL DATA THROUGH VIDEO DEVICES 26–27 (2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf [https://perma.cc/4X83-NLD6].

34. *See infra* notes 42–43 and accompanying text (discussing the problems unfolding with the implementation of Apple's privacy labels).

35. *See* Axel Marx, *Global Governance and the Certification Revolution: Types, Trends and Challenges*, *in* HANDBOOK ON THE POLITICS OF REGULATION 590, 598 (David Levi-Faur ed., 2013).

36. *Id.*

environment-related information of minor and limited significance to mask more consequential omissions and failings.[37]

Output legitimacy, or the lack thereof, pertains to weak enforcement mechanisms ensuring accurate reporting in the label. When the condensed disclosure is made by a firm itself, such accuracy might be compromised because of self-interests. Studies have reported substantial trends of false reporting regarding certification and meeting privacy standards.[38] Therefore, as in other domains, such as nutrition and eco-labeling, intermediation by a third party appears to be more prudent.

To better understand the above concerns and the distinctions between them, consider a recent review of Apple's "privacy nutrition labels" initiative.[39] This initiative called on firms to select their appropriate privacy setting from existing menus.[40] The result is a standardized label intended to convey, in simple form, basic privacy issues to the public.[41] For instance, the label "Data Linked to You" presents through clear icons whether the collected information that might be linked to one's identity pertains to purchases, contact information, location, etc. Similar icons are provided for a label addressing "Data Used to Track You" across apps owned by other companies.[42]

37. *See* James. P. Nehf, *Regulating Green Marketing Claims in the United States* (Ind. Univ. Robert H. McKinney Sch. of L. Working Paper, Paper No. 2018-9, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240164 [https://perma.cc/429T-RA5B].

38. Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEGAL STUD. S13, S16, S37 (2016).

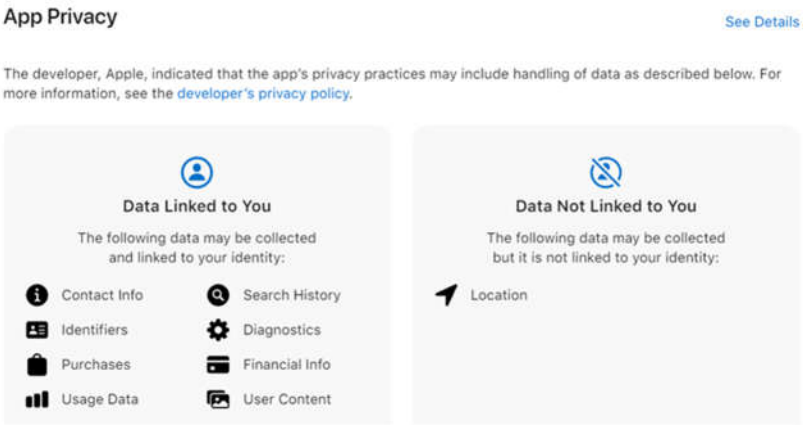
39. Geoffrey A. Fowler, *I Checked Apple's New Privacy 'Nutrition Labels.' Many Were False.*, WASH. POST (Jan. 29, 2021), https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/ [https://perma.cc/8MPF-J7LF].

40. *See id.*

41. Melanie Weir, *What Are Apple's Privacy Nutrition Labels?: Here's What You Need to Know About the New App Store Feature That Prioritizes User Privacy*, BUS. INSIDER (Jan. 20, 2021, 1:22 PM), https://www.businessinsider.com/what-are-apple-privacy-nutrition-labels [https://perma.cc/J92V-2X6Q].

42. *See* Illustration, which pertains to one of Apple's own products, the App Store application.

Illustration: Privacy Labels for Apple App Store[43]



This labeling scheme appears promising. At the same time, a recent review indicated that firms constantly misrepresented their privacy practices, making them appear more favorable than they really were, although it is unclear whether this was intentional or rather resulted from negligence or even an error in good faith on the part of the firm.[44] Note that in this particular labeling scheme, the labeling formats were designed by an external party (Apple), mitigating concerns of input legitimacy (that is, that firms would selectively decide what to reveal and how). Still, self-reporting undermined the scheme's output legitimacy.

In his discussion of intermediation, Reidenberg was well aware of the shortcomings of self-reporting and pointed out several types of third parties that could act as trusted intermediaries.[45] Government may be a natural choice, as was the case in some early data protection intermediation schemes.[46] But with the number of digital entities interacting with the public growing exponentially, scalability becomes a challenge, and this task exceeds the capacities of government.[47] For such an extensive task, private forms of intermediation must take center stage, with the government developing standards for their operation.[48] Alternatively, the government

43. *Privacy*, APPLE, https://www.apple.com/privacy/labels/ [https://perma.cc/37NK-8N6A] (last visited Feb. 2, 2022).

44. *See* Fowler, *supra* note 39.

45. Reidenberg et al., *supra* note 9, at 1424.

46. *See* Johanna Carvais-Palut, *The French Privacy Seal Scheme: A Successful Test*, *in* PRIVACY AND DATA PROTECTION SEALS. *supra* note 28, at 49 (discussing scheme applied in France); Marit Hansen, *The Schleswig-Holstein Data Protection Seal*, *in* PRIVACY AND DATA PROTECTION SEALS, *supra* note 28, at 35 (discussing scheme applied in the German federation of Schleswig-Holstein).

47. *Id.* at 100 (indicating that today, very few schemes are owned or operated by the government).

48. *See* Reidenberg et al., *supra* note 9, at 1416.

could merely certify or supervise the intermediaries and the standards they developed on their own.[49]

Beyond the intermediation process, let us now consider its form. In the simplest scenario, the intermediated content—such as a label—could convey merely a binary signal of meeting or not meeting a certain standard, which might be set by a firm or a government (for example, compliance with the General Data Protection Regulation (GDPR)). Indeed, a notice of EU data protection compliance has existed for some time; recently, the process of GDPR compliance certification has been incorporated into the GDPR's regulatory framework,[50] but it has failed to create sufficient traction so far.[51] Yet, to achieve the noted objectives of user empowerment, additional nuances of privacy-related practices must be reported beyond a mere binary signal.[52] To intermediate effectively and efficiently, third parties must supplement firms' privacy policies with a simplified, yet data-rich, signal. Nuanced—as opposed to binary—intermediation can take various forms. This Essay focuses on labels, which might include several accepted formats selected from a predefined menu. For example, Apple's privacy nutrition label includes several privacy-related parameters.[53]

Given the fact that a variety of intermediaries may be entering the digital domain,[54] prudent actors would be wise to devise and use *universal* labeling formats. Reidenberg and his coauthors strongly emphasized the importance of universal formatting, noting that diversification of intermediation notification formats would result in an unworkable reality:[55] there would be too many ways in which adherence to privacy, or the lack thereof, could be conveyed. Alas, such splintering in intermediation is currently taking place and is likely to intensify.[56] If every intermediary or every firm, when

49. *See* Marx, *supra* note 35 (addressing various options for entities developing the schemes, distinguishing between companies, sector organizations, and independent organizations).

50. Regulation 2016/679, General Data Protection Regulation, arts. 42, 43, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]. *See generally* Reidenberg et al., *supra* note 9 (certifications indicate compliance with GDPR principles).

51. For more on this issue, see Eric Lachaud, What GDPR Tells About Certification (March 19, 2020) (unpublished manuscript), https://ssrn.com/abstract=3557167 [https://perma.cc/EES8-Z8TN]. Note that the relevant page indicating EU certification is empty. *Register of Certification Mechanisms, Seals and Marks*, EUR. DATA PROT. BD., https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en [https://perma.cc/ZT4N-V86P] (last visited Feb. 2, 2022).

52. For an opposing view regarding the risks of shifting beyond a binary signal, see Shmuel I. Becher, *A "Fair Contracts" Approval Mechanism: Reconciling Consumer Contracts and Conventional Contract Law*, 42 U. MICH. J.L. REFORM 747, 765–67 (2009) (surveying potential challenges by grading consumer contracts on a numeric scale).

53. Ian Carlos Campbell, *Apple Will Require Apps to Add Privacy "Nutrition Labels" Starting December 8th*, VERGE (Nov. 5, 2020, 8:42 PM), https://www.theverge.com/2020/11/5/21551926/apple-privacy-developers-nutrition-labels-app-store-ios-14 [https://perma.cc/M2SH-NEM7].

54. *See* PRIVACY AND DATA PROTECTION SEALS, *supra* note 46, at 106 (indicating the fragmentation in the intermediation market).

55. *See* Reidenberg et al., *supra* note 9, at 1429.

56. *See also* Kamara & De Hert, *supra* note 28, at 21.

applying their own labels and icons, uses a different format and methodology for their aggregated and abridged disclosures, diversification follows. In this reality, users must learn to glean the meaning of the various labels, tables, and summaries—and their relevant nuances—to understand firms' privacy practices and compare them. Even with intuitive disclosure formats, such a taxing comprehension task would prove inefficient and time-consuming, if not intolerable.[57] Labeling standards are, therefore, of the essence.

Commercial entities may step in to develop and provide disclosure standards, but this might prove problematic because of reliability concerns,[58] leading back to the government option for developing uniform labeling templates (with possible assistance from academia). The government option also benefits from its advantage in collecting and aggregating relevant information that is produced by various entities operating in this space and that would be used to develop the label.[59] Similar dynamics have developed in energy consumption and nutritional labeling.[60]

In sum, intermediated disclosure is important and best achieved by a trusted third party attending to it. Moreover, intermediation by labeling is best carried out in a unified and nuanced form. Yet, even if labeling meets these requirements, achieving output legitimacy and, thus, effective intermediation is far from simple. This is the challenge that Reidenberg's recent work sought to address while examining possible measures that take advantage of current interconnectability and advanced technology.

2. Reidenberg on Accurate Labeling Challenges and Responses

The above mapping presents a general blueprint of how we may successfully bridge the vast texts of privacy policies and the marginally interested, but attention-deprived, public. It appears, however, that current initiatives to meet this bridging task have failed.[61] Reidenberg and his team identified several key challenges that may explain such failure and endeavored to resolve them.[62] The backdrop for this analysis is the recognition of the *immenseness* undermining the privacy intermediation task.

---

57. This concern is noted in other certification areas as well. *See* Marx, *supra* note 35, at 600 (noting the problems of fragmentation in the certification sphere).

58. Reidenberg et al., *supra* note 9, at 1437. This point was made early on by A. Michael Froomkin. *See* Froomkin, *supra* note 14, at 1526.

59. For a discussion of the advantages of the government in collecting information from diverse segments of the cybersecurity sector and in facilitating such collection, see Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. REV. 515, 551–52 (2017).

60. *See* Reidenberg et al., *supra* note 9, at 1420–21. For a discussion of the various strategies for regulating labels in the area of nutrition, see Shmuel Becher et al., *Hungry for Change: The Law and Policy of Food Health Labeling*, 54 WAKE FOREST L. REV. 1305 (2019).

61. Marotta-Wurgler, *supra* note 38, at S15 (noting that, as of 2016, only about a quarter of leading websites publicized compliance with a certificate).

62. *See* Reidenberg et al., *supra* note 9, at 1428–33 (addressing problems); *see also id.* at 1441 (addressing possible solutions).

Intermediation calls for reading, comprehending, analyzing, and successfully conveying the contents of privacy policies. The vast number of websites, as well as the lengths of the legal texts and their vagueness, complexity, and difficulty, which often require specific expertise to unravel, all lead to an insufferable project that is too onerous for ordinary humans to undertake. To meet the immense challenge of decoding privacy notices, Reidenberg's team discussed the feasibility of applying two great forces that modern technology has enabled: crowdsourcing and automation. As I now detail, they identified substantial, but workable, problems with both. To reach these conclusions, Reidenberg and his teams carried out two rigorous multilevel empirical studies examining the nature of privacy notices, particularly the degree of their ambiguity and vagueness.[63] The invaluable insights revealed in these studies explain why privacy policy intermediation presents a unique challenge, even when applying novel methods.

In one study, published in *The Journal of Legal Studies*, Reidenberg and his team examined privacy policies linguistically to establish whether vague language compromised the semiautonomous process by which they conducted the privacy policies' analysis.[64] This examination demonstrated that the policies' texts were filled with conditional and modal terms.[65] Such terms are a clear indication of vagueness that injects inaccuracy into an automated or even semiautomated intermediation process. In yet another empirical study, published in the *Berkley Technology Law Journal*,[66] Reidenberg and his colleagues confirmed the inherent vagueness of privacy notices by showing discrepancies between how experts and users understood several key privacy policies, as well as discrepancies between understandings within each of the tested groups.[67]

Based on these insights, Reidenberg turned to both crowdsourcing and automation to examine their potential role in privacy policy intermediation. In theory, crowdsourcing solves some of the challenges presented by the immensity of the problem and enables intermediation. According to one popular definition, crowdsourcing refers to "the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community."[68] The task of reading and comprehending privacy policies in their entirety and on a grand scale seems impossible, but it may be possible to carry it out collectively by distributing it among the millions of online users interacting with the relevant data aggregators. Here every such user will be performing a minimal task while contributing to an aggregated resource. This resource would provide

63. *See id.* at 1434; *see also* Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S165 (2016).

64. *See generally* Reidenberg et al., *supra* note 63, at S163.

65. *Id.* at S169–70.

66. Reidenberg et al., *supra* note 11, at 39.

67. *See id.*

68. *Crowdsourcing*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/crowdsourcing [https://perma.cc/QTV9-CBVK] (last visited Feb. 2, 2022).

many other users with summaries and trusted recommendations, which, again, may be premised on a uniform label.[69]

Crowdsourcing, however, has a checkered history. Early on, it was hailed as promising a novel production method that may even successfully compete with that of "the firm."[70] Yet, subsequent sobering analyses have shown that, in many circumstances, the crowdsourcing dynamic—or similarly, the reliance on an "open commons"—does not provide adequate results leading to the successful conclusion of complex tasks.[71] Some of the analyses indicated that even when proven successful, the studied dynamic did not involve crowdsourcing in its purest form but included some forms of economic compensation or other property rights.[72] Reidenberg feared that crowdsourcing would fall short in the area of privacy policy comprehension and subsequent intermediation, and as shown below, even the most avid supporters of the power of peer production may agree.

According to a popular conceptualization of the peer production process, it is made possible, among other reasons, by allocating overlapping granular tasks to the masses.[73] In the case of privacy policy, every participant in the crowdsourcing initiative receives a manageable task: a small portion of a privacy policy to review, summarize, and report on. Subsequently, the technological infrastructure would aggregate the results into a broad recommendation system, introducing some crucial redundancy to double-check reviewers for errors and biases. Unfortunately, this method is likely to fail for reasons that Reidenberg has proven empirically.

In their experiments, Reidenberg and his team found that different users understand the same privacy-related texts quite differently.[74] This finding undermines the precision of a crowdsourced aggregated privacy grade or evaluation, especially if it consists of an average of polarized views regarding the meaning of contractual statements in privacy policies.[75] Therefore, even assigning overlapping granular tasks to many users would not lead to an

69. For a recommendation of the use of crowdsourcing to meet the intermediation challenge, see Johanna Johansen et al., *A Multidisciplinary Definition of Privacy Labels: The Story of Princess Privacy and the Seven Helpers* 17 (2021) (unpublished manuscript), https://arxiv.org/pdf/2012.01813.pdf [https://perma.cc/8BNJ-7WTW].

70. Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 372 (2002).

71. For an in-depth analysis of the inability of commons-like models to overcome various vast tasks, see generally Jonathan M. Barnett, *The Illusion of the Commons*, 25 BERKELEY TECH. L.J. 1751 (2010). *See also* Megan Wu, *Quirky, the Failure of Invention Crowdsourcing*, HARVARD BUS. SCH. DIGIT. INITIATIVE (Feb. 2, 2017), https://digital.hbs.edu/platform-digit/submission/quirky-the-failure-of-invention-crowdsourcing/ [https://perma.cc/N3UH-FABC] (discussing the failure of "Quirky," a platform for invention crowdsourcing); Paul Clough et al., *Examining the Limits of Crowdsourcing for Relevance Assessment*, 17 IEEE INTERNET COMPUTING, no. 4, 2013, at 32.

72. *See generally* Rochelle Cooper Dreyfuss, *Does IP Need IP?: Accommodating Intellectual Production Outside the Intellectual Property Paradigm*, 31 CARDOZO L. REV. 1437 (2010).

73. *See* Benkler, *supra* note 70, at 379, 435.

74. *See* Reidenberg et al., *supra* note 9, at 1436; *see also* Reidenberg et al., *supra* note 11, at 86.

75. *See* Reidenberg et al., *supra* note 9, at 1432.

adequate outcome because the inputs received from users would be too far apart. Furthermore, the task at hand seems too complicated for the average online reader. Thus, the number of potential reviewers is likely to be insufficient to provide meaningful feedback for the many relevant websites and their policies. Reidenberg noted that the enormous size and complexity of the task is reflected in the limited feedback on privacy notices currently available.[76] Accounting for all these elements leads to the conclusion that, alone, a review process based on crowdsourcing is unsustainable. Some of these challenges, however, might be addressed through *automation*.[77]

In theory, highly advanced methods, such as those of natural language processing (NLP), can quickly peruse the lengthy privacy policies, analyze the text, and provide users with summaries or an assessment of whether the policy meets users' or the intermediary's predefined preferences. The results of this analysis can be conveyed using the standardized forms of intermediation. These techniques hold the promise of coping with the vast amounts of text concerning privacy policies, as has been achieved with remarkable success in a variety of legal and other areas.[78]

Automation, however, is far from a panacea in this case. Although it appears attractive in theory, in practice, matters are not so simple. For example, Reidenberg and his team uncovered systematic faults that they believed would render automated "reading" and intermediation of privacy policies excessively difficult.[79] Like the crowdsourcing topic above,[80] this

76. *See id.* at 1430.

77. For a discussion of an automated tool for benchmarking and its shortcomings, see Yonathan A. Arbel and Shmuel I. Becher, *Contracts in the Age of Smart Readers*, GEO. WASH. L. REV. (forthcoming 2022) (manuscript at 20–21), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3740356 [https://perma.cc/G6K8-KFYL]; *see also* SEBASTIAN ZIMMECK & STEVEN M. BELLOVIN, USENIX: THE ADVANCED COMPUTING SYS. ASS'N, PRIVEE: AN ARCHITECTURE FOR AUTOMATICALLY ANALYZING WEB PRIVACY POLICIES 1 (2014) (discussing a model for ranking privacy policies based on the inclusion and exclusion of terms).

78. For instance, some AI tools were able to successfully annotate nondisclosure agreements (NDAs), surpassing the abilities of lawyers engaged in a similar task. *See LawGeex Hits 94% Accuracy in NDA Review vs 85% for Human Lawyers*, ARTIFICIAL LAW. (Feb. 26, 2018), https://www.artificiallawyer.com/2018/02/26/lawgeex-hits-94-accuracy-in-nda-review-vs-85-for-human-lawyers/ [https://perma.cc/HG9Y-7VKE]. For a critical discussion of models for analyzing consumer contracts, see Noam Kolt, *Predicting Consumer Contracts*, 37 BERKELEY TECH. L.J. (forthcoming 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3844988 [https://perma.cc/VES4-T298]. For a discussion of the internal and external risks of automated reading, see Arbel & Becher, *supra* note 77.

79. *See* Arbel & Becher, *supra* note 77. In this paper, the authors noted additional problems and concerns related to the use of smart readers for reviewing online contracts, such as their vulnerability to adverse "attacks," in which text drafters used various methods to "trick" the scanning and "reading" algorithm into grading their texts positively, even if this was not deserved. *Id.* At this time, I do not find this concern to be substantial. Many of the attack schemes noted by Arbel and Becher amount to fraud, exposing their perpetrators to substantial liability if discovered and made public by interested parties. *See id.* For this reason, I expect such attacks to be rare. Another concern noted was that these processes are driven by "black boxes" and therefore cannot be explained after the fact. But, because these initiatives are intended to be governed by trusted third parties or by the government, accountability-based safeguards could be built in, limiting this concern. *Id.* at 30–33.

80. *See supra* notes 64–72 and accompanying text.

argument follows from the vagueness and ambiguity of privacy policies.[81] Reidenberg found that trained experts have provided conflicting responses when attempting to explain the meaning of privacy policies, rendering reliance on machine-based learning, which would arguably be inferior to that of experts, doubtful.[82]

According to Reidenberg, however, not all is lost. He offered solutions, insights, and several silver linings that may enable effective and streamlined intermediation for privacy policies. Based on the noted analysis, he and his team identified key parameters for predicting when automation and crowdsourcing may nevertheless succeed, and by contrast, when they will utterly fail.[83] For example, they argued and proved that reliance on governmentally preapproved texts in privacy policies could limit problems of intermediation and should be adopted and therefore encouraged whenever possible.[84] These texts would be easier to sort and intermediate through automation, crowdsourcing, or both.

Furthermore, rather than relying exclusively on crowdsourcing or automation, Reidenberg and colleagues recommended applying hybrid systems in which *both* machines and human annotators play a role.[85] They further clarified that the tasks presented must be unambiguous, which could help limit disparities between respondents.[86] Finally, they advocated for ongoing examination of the differences in the interpretation of privacy policies between experts and users, as well as a continued examination of the disparity in such understanding within the groups of users and experts themselves.[87] The results of this examination have the potential to provide an indication of whether the outcomes of such a hybrid process could be relied upon as a form of effective and accurate intermediated notice and, when applicable, labeling.[88]

It should be noted that since the publication of Reidenberg's (and his collaborators') projects, automated processes powered by artificial intelligence and machine learning have continued to evolve and potentially improve. Recent publications address attempts to automatically analyze

81. *See* Reidenberg et al., *supra* note 11, at 83–84.

82. *See id.* at 87.

83. For example, they show that for location data, individuals can grasp the privacy issues discussed in the notices, which could therefore be properly captured by an automated process as well. *See id.* at 85–86; *see also* Reidenberg et al., *supra* note 63, at S184.

84. *See* Reidenberg et al., *supra* note 63, at S181.

85. *See id.* at S184. For reviews of other projects analyzing privacy policies that required similar hybrid approaches, see SHUANG LIU ET AL., HAVE YOU BEEN PROPERLY NOTIFIED?: AUTOMATIC COMPLIANCE ANALYSIS OF PRIVACY POLICY TEXT WITH GDPR ARTICLE 13 (2021); RAZIEH NOKHBEH ZAEEM & K. SUZANNE BARBER, COMPARING PRIVACY POLICIES OF GOVERNMENT AGENCIES AND COMPANIES: A STUDY USING MACHINE-LEARNING-BASED PRIVACY POLICY ANALYSIS TOOLS 29, 38 (2021).

86. This may be achieved by regulating the language of privacy policies, either by using predefined texts, simple texts, or recognized "logic" symbols or terms.

87. *See* Reidenberg et al., *supra* note 11, at 88.

88. Such hybrid methods create substantial challenges resulting from human overreliance on automated decisions. For a discussion of these challenges and their possible solutions, see Danielle K. Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305 (2008).

privacy policies and indicate some level of success.[89] For instance, one study compared governmental and commercial privacy policies and found the former to be, on average, more protective than the latter—a finding which is clearly aligned with intuition.[90]

It is therefore possible that, within a few years, effective, accurate, and informative standardized automated intermediation will become a reality. Such technologies might prove to be "game changers." For instance, they might render standardization efforts unnecessary, as one system might be able to provide every user with an intermediated experience pertaining to everything the internet has to offer. If this technology would prove effective and available, the nature of privacy policies might also change, requiring the rethinking of much of the discussion noted above. The analysis that follows does not, on the whole, account for this tectonic change (although it acknowledges the questions that will remain in place at some junctures). The full analysis of such technologies must thus wait until the technologies provide clear indications of competence and success.

Part I discussed the promises and serious challenges of privacy intermediation schemes, focusing on possible structural measures to achieve acceptable levels of input and output legitimacy when formulating labels. Admittedly, the discussion set aside substantial scholarship adhering to doctrines regarding the proper way to design the label and, instead, focused on institutional aspects of the intermediation process. But, both the design of the label itself and the nature of the interaction with the users call for broader policy decisions. Next, Part II addresses some of these issues in view of Reidenberg's work.

II. TAKING REIDENBERG SERIOUSLY: DESIGNING WORKABLE SMART DISCLOSURES

Disclosure has become a popular policy response on one hand and a popular target of scholarly criticism on the other. In this part, I propose to integrate Reidenberg's intermediating disclosure model into the broader discussion of disclosure. Relying on other aspects of Reidenberg's scholarship, such integration will ensure the smooth and accurate operation of intermediation. Indeed, for innovative intermediation to succeed, we must attend to several crucial design decisions regarding the intermediary user interface, including establishing and meeting the objectives, priorities, and confines of disclosure. This part also discusses personalized privacy notices and the potential pitfalls of such a disclosure strategy, given the insights presented above.

89. *See* ZAEEM & BARBER, *supra* note 85; LIU ET AL., *supra* note 85 (detailing various studies relying on AI and machine learning to automatically analyze privacy policies).

90. *See* ZAEEM & BARBER, *supra* note 85, at 39.

A. Basic Smart Labeling Design Decisions: *Objectives and Priorities*

Reidenberg's innovative disclosure strategies are focused on condensing much of the relevant privacy-related information into a standardized and simple format, or *label*.[91] Such strategies have been used, with varying success, in other areas, including food, energy, finance, and environmental protection.[92] In the field of privacy, there have been some promising proposals, mostly from academia, promoting labeling, including some early prototypes.[93] Such measures were also noted by U.S. regulators contemplating the regulation of privacy[94] and by tech giants considering self-regulation.[95] Reidenberg and his colleagues explain that, in the case of privacy, a governmental entity, such as the Federal Trade Commission (FTC), should be charged with the task of creating such labels and their criteria.[96] Such an entity would specify "both what factors are to be considered—privacy practices and specific data points and how each of these aspects is to be judged and weighted."[97] Yet, beyond the identity of the designing entity, a variety of other decisions are required, which vary based on: (1) the main *objective* of the disclosure and (2) the *priorities* set between its various goals.

1. Intermediation Objectives

Earlier academic discussions regarding intermediation via labeling feature crucial lessons for concrete privacy-related labeling schemes. In this Essay, I focus on Professor Richard Craswell's work, which addressed the broader realm of disclosure requirements in contractual and administrative contexts.[98] In his scholarship, Craswell closely examined several instances in which governments set in place disclosure formats, as well as the various issues that ensued.[99] Craswell made two crucial points. First, he emphasized that when governments formulate disclosure policies through ranking or labeling, they must initially establish what they seek to achieve, then move to do so.[100] This obvious point is sharpened by the observation that labels and their design are not neutral and therefore must strive to achieve a given objective. In other domains, such design-driving objectives included the lowering of gas emissions or limiting human consumption of calories or saturated fat.

---

91. *See* Reidenberg et al., *supra* note 9, at 1441.
92. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 122, 136.
93. *See* KELLEY ET AL., *supra* note 29.
94. *See* Waldman, *supra* note 2, at 149–50.
95. *See* Campbell, *supra* note 53.
96. *See* Waldman, *supra* note 2, at 182.
97. Reidenberg et al., *supra* note 9, at 1441.
98. *See* Richard Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere*, 92 VA. L. REV. 565, 579 (2006).
99. *See id.* at 581–83. On the complexities of labeling, see BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 126.
100. *See* Craswell, *supra* note 98, at 588.

In the area of privacy, formulating a disclosure objective may seem like a nonevent. Disclosure and notice are assumed to be put in place to "empower data subjects" and enable their effective choices, as per Reidenberg's definition adopted above and the objectives it includes.[101] In the case of privacy, disclosure is a measure serving and promoting a fundamental right, as opposed to an instrumental objective. Therefore, there is no need for additional focus when formulating proper disclosures.[102] Yet, even fundamental values, such as privacy, have nuances and priorities. Thus, Craswell's insights call for both a clear mapping of the forms of given cognitive processes that the contemplated disclosure policies should enable and the crafting of them accordingly.

To explain and understand the implications of this design decision for privacy, let us return to the nature of labels. In his work, Craswell introduced the contrast between comparison and stand-alone assessment in the use of labels and supervised disclosure.[103] When structuring privacy labels or other forms of sophisticated disclosure, we must decide whether they must facilitate an effective *comparison* of privacy practices between firms (also referred to as a "benchmarks")[104] or a better *understanding* of what firms do with our personal data.[105] Here, it is possible to argue that we should have both and simply ignore this issue.[106] Yet, human attention is a zero-sum game; therefore, it is preferable that at every juncture one objective be selected and given preference.

As Craswell explained, the noted objectives (comparison and understanding) are in direct conflict.[107] Consider the context of environmental protection: the Environmental Protection Agency (EPA) introduced the miles-per-gallon (MPG) ratings for vehicles.[108] Craswell explained that, on its own, the MPG parameter was often completely erroneous and did not accurately reflect the mileage achieved by vehicles (per gallon).[109] But, the error was systematic for all tested vehicles.[110] Therefore, the MPG rating proved highly effective because it allowed a comparison between similar vehicles and their relative contribution to

101. *See supra* note 25 and accompanying text.

102. Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1530.

103. *See* Craswell, *supra* note 98, at 586 (distinguishing between absolute and relative information).

104. *See* Arbel & Becher, *supra* note 77, at 19.

105. For another discussion of the relationship between comparative and other forms of disclosure, see Waldman, *supra* note 2, at 180.

106. Indeed, several recent articles addressing label design distinguished between these objectives but noted that they both should be promoted. *See* RAILEAN & REINHARDT, *supra* note 19, at 26–27; Johansen et al., *supra* note 69, at 14.

107. Craswell, *supra* note 98, at 585.

108. *See id.* at 581–82.

109. *See id.* at 588.

110. *See id.* ("In particular, as long as the ratings accurately depict the relative efficiency of different models, they might still be perfectly adequate to give manufacturers an incentive to try to improve their cars' performance.").

pollution, which was, arguably, the objective these regulations sought to achieve.[111]

In other domains, comparison-driven disclosure is less helpful or might even prove harmful. For example, Craswell pointed to instances in which regulators banned tobacco companies and cigarette distributors from asserting comparative claims about the amount of tar in various cigarettes as opposed to the amount in their competitors' cigarettes.[112] Regulators feared that such comparative claims would undermine the overall strong message concerning the negative consequences of smoking.[113] In such cases, labels should be constructed to focus attention on the ultimate effect of use rather than its relative one.

Returning to the framing of labeling and disclosure policy for privacy interests leads to a difficult dilemma concerning the need to identify the proper emphasis in such intermediated disclosure: should the emphasis be on regulations that promote simple comparisons between websites or rather on those that promote the understanding of the "stand-alone" privacy value that each website and experience provides? Intuitively, the privacy context mandates focusing on "stand-alone" disclosures. The label should provide greater insights about the firm's concrete privacy practices, even at the cost of complicating the ability to engage in a comparison between similar firms. This position has the greatest merit when the individual's autonomy might be compromised, as regarding health, speech—in the case of social networks, for instance—or finance. The greater the autonomy interest, as in the case of health-related information, the stronger the justification for providing independent assessments of the policy. At such points, comparisons might only confuse individuals, leading them to erroneously believe that the subpar data practices they are subjected to are acceptable because they are better than those offered by others in the same industry.[114] Nevertheless, comparison-focused labeling may be the preferred policy option for consumer websites in vibrant e-commerce markets, given the prospect of competition.[115]

2. Intermediation and Prioritization

Returning to the general scholarship on information disclosure leads back to Craswell's second intuition, which relates to the importance of prioritization.[116] This notion focuses on an obvious benefit of a labeling

111. *See id.* at 588.
112. *See id.*
113. *See id.* at 590.
114. Although a comparative view may indeed empower users even when limited competition is available, the detriments of presenting comparative advantages as achievements are substantial.
115. For some early evidence of competition between firms regarding privacy matters, see Marotta-Wurgler, *supra* note 38, at S37.
116. *See* Craswell, *supra* note 98, at 577 ("In short, there is a lot of information about every contract that might conceivably be disclosed. As a practical matter, though, disclosing all of this information is impossible. As a result, any disclosure rule will have to prioritize: It will

scheme: that it succinctly presents all relevant information. But, this comes at a price. Disclosure design is not only about requiring the publication of certain information. Rather, it requires hard decisions about *which* forms of information should be prioritized and presented saliently. In the words of Craswell, "there is generally far more information that *might* be disclosed than it would ever be possible to communicate."[117] For example, when mandating nutrient disclosure, the government requires the publication of the nine most important ones, rather than allowing for greater discretion for manufacturers to list numerous items.[118] The fear here is that providing excessive flexibility might allow the obfuscation of the problematic elements, hiding them from the public.[119]

This prioritization challenge is of particular relevance to labeling initiatives in the area of privacy. If left unchecked, the most pertinent and important aspects of privacy and information management policies might be buried under other unimportant verbiage. In other words, firms might manipulate disclosures to hide the most damning aspects of their operation. Furthermore, there might be many important elements that firms and regulators would want to disclose, but the interests of the two might not be aligned. Deciding which facts are most important for disclosure requires an elaborate decision-making process, which is crucial for establishing a uniform labeling standard in matters of privacy.

Achieving proper prioritization and devising a protocol for doing so calls for difficult and context-specific decisions.[120] In matters of privacy, this requires distinguishing between the two separate disclosure objectives noted above: enhancing autonomy and facilitating competition.[121] In most cases, disclosures should focus on autonomy and empowerment. Therefore, the labels should provide—almost exclusively—information on issues that are central to the individuals' rights and their ability to control their data—or, at least, an aggregated version of such preferences that account for the majority of citizens or users.

Three prioritization methods, or their combination, may be considered to meet the prioritization challenge. First, prioritization may be determined by a normative analysis. In this case, it would be driven by what regulators find to be the most important aspects to consider and the easiest to understand, perhaps influenced by academic thinkers in doing so and, naturally, by lobbying and other interested parties that would influence the outcome. Second, the inquiry aiming to prioritize may be "positive," that is, driven by

---

have to distinguish those attributes of the contract that are worth disclosing from those that are not.").

117. *Id.* at 575.

118. *See id.* at 577.

119. *See id.* Note that since the writing of that article, governments worldwide have introduced a range of health and food labels. *See* Becher et al., *supra* note 60, at 1323–44.

120. Yet another problem that might develop is that when only part of the elements gains public attention, competition between firms focuses on their improvement, as opposed to other "hidden" elements. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 176.

121. These two objectives were also noted by Ben-Shahar and Schneider. *See id.* at 5, 36.

the public's opinion and preference. Thus, the factors could be established based on surveys. The field of privacy famously features a disparity between these normative and positive elements, often referred to as the "privacy paradox." Therefore, reliance on any one of them can generate controversy.[122]

In the face of these difficulties, perhaps a third option should be explored. This is a somewhat modified version of the previous "positive" method, and it focuses on the elements that the public, through its access to the legal and regulatory system, is signaling to be of interest. As opposed to surveys, the outcome here would provide a stronger indication of interests, which, given the aspects of regulatory selection, have a normative dimension as well. These interests could be identified by tracking privacy-based litigation and regulation measures and identifying the themes most frequently addressed in the claims presented, as evident in the relevant legal documents. Research premised on this methodology was indeed carried out by Reidenberg, in his study from 2015, which also integrated elements of the first, normative aspects.[123] Thus, adopting this option would allow for reliance on yet another important strand of Reidenberg's work to promote an overall effective privacy labeling scheme.

In the mentioned study, and in an attempt to provide a focal point for privacy labels, Reidenberg and his team worked through the relevant case law and regulatory history.[124] In the course of this work, they identified four key issues addressed in privacy-related litigation and regulatory enforcement measures: (1) informing the public about the prospects of unauthorized disclosure, (2) surreptitious collection (with respect to the information collected and the duration of its retention), (3) insufficient security, and (4) excessive retention of data.[125] Subsequently, they turned to examine themes that could be conveyed most effectively, thereby adding a normative dimension to the discussion. They concluded that labeling should focus on the first two themes—unauthorized disclosures and surreptitious collection—as opposed to the last two, which would not be properly understood by disclosure and were therefore unfit for labeling.[126]

Reidenberg's methodology, which calls for reliance on salient litigation and regulator-inquiry themes as indicators of prioritizing in labeling, has a strong intuitive appeal and provides instrumental value. Following this analytical strategy would ensure that the information needed for litigation or regulation indeed reached those seeking to initiate these processes, whether private parties or public servants, given the noted emphasis in the disclosure process. This prioritization method is not without faults, however. Focusing

122. The "privacy paradox" possibly demonstrates the disparity between actual preferences and the positions people *should* take regarding their personal information. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021) (critiquing the notion that such disparity exists).

123. *See generally* Reidenberg et al., *supra* note 14.

124. *See id.* at 518–23.

125. *See id.* at 488.

126. *See id.* at 517–24.

the public's attention on the above elements, through disclosure, would most likely prove biased toward certain information (given the specific claims) while neglecting others. It would, therefore, lead to an emphasis on information facilitating "practical" claims, while obscuring knowledge-promoting abstract claims and concerns that do not have clear monetary implications and thus do not implicate substantial litigation and regulatory measures. Furthermore, it might also be tilted toward the interests of wealthy and sophisticated users, given their resources and ability to bring legal actions, in turn influencing the contents of the legal docket.[127] A possible response to this critique is that such biases could be cured by changes in court rulings and regulations. With such changes, the legislative and regulatory map would also change over time and, with it, the disclosure priorities. Yet, these changes might come too late and be too limited. Therefore, norm-based considerations aiming to compensate for this potential bias must be part of the specific methodology used to prioritize disclosure.

The labeling strategies that focus on autonomy and empowerment must lead the way, but at certain junctures, they should be supplemented by attempts to promote the objective of norm-based competition between firms. There is some initial evidence indicating heightened levels of privacy in the presence of competition—for example, in the case of adult websites.[128] Such evidence—and the hope that competition may enhance privacy in certain instances—calls for identifying the limited cases[129] in which competition between firms is sufficiently fierce so that privacy consideration may be rendered salient. In these cases, firms would cater to their consumers' privacy preferences. Here, labeling should focus on the privacy-related elements that firms might "compete" over, similar to the way car manufacturers compete over providing higher MPG.[130] Relevant areas for disclosure should be identified by additional testing and research. Intuitively, they may include labeling information pertaining to the sharing of personal data with third parties and limitations on collection data points that individuals deem as sensitive and that are possibly drivers of competition between firms.

B. Personalized Disclosures: A Cautionary Note

The discussion so far assumes that intermediated privacy notices and labels would be distributed in uniform fashion—that is, all users would receive the same information in the same format. Recently, however, academics have begun promoting the notion of personalized disclosures to

127. Note that this particular concern for bias may be eased by class actions, which may bring the voice of the masses to the forefront, and by regulatory focus on weaker social segments.

128. *See* Marotta-Wurgler, *supra* note 38, at S37.

129. *See supra* note 115 and accompanying text.

130. *See Fuel Economy Government*, U.S. DEPT. OF ENERGY, https://www.fueleconomy.gov/ [https://perma.cc/Q9V8-WNXV] (last visited Feb. 2, 2022) (providing MPG comparisons).

be tailored to individual persons, premised on their relevant personal traits and projected preferences, and powered by big data.[131] In theory, regulators may formulate lists of privacy-related priorities for various demographics (age, gender, domicile), relying on the prioritization methodologies noted above: normative, based on surveys, or derived from litigation for the particular social segment to which the user belongs. They may even provide some users with comparative information and others with an independent, stand-alone factor. To further perfect the process, users should be able to opt out of the category into which they were placed and signal different disclosure preferences if they believe they have not been properly classified.[132]

On its face, a personalized label with different salient elements for every individual would offer greater utility with respect to privacy. With such personalization in place, the information every attention-deprived user receives would be of greater accuracy and relevance, resulting in an optimal outcome. Yet, such schemes raise substantial enforcement challenges and might actually not be advisable when it comes to privacy.[133] This concern is based on the fact that the interests of the entity governing the disclosures—ideally a trusted third party supervised by the government—and the disclosing parties are often unaligned: the latter might be trying to hide from their users certain segments of information, which the former may wish to disclose.[134] With such personalization in place, therefore, it would be extremely difficult for an external auditor to track whether all individuals are receiving appropriate disclosures. It would also be difficult to examine whether the label and the relevant firm's full privacy policy match. Finally, after the fact, it would be almost impossible to track whether firms have abided by the concrete (and abridged) privacy-related promises they made to every user.

As noted above, with respect to privacy, the intermediation challenge has grown too vast and complex to be carried out by a central, human-operated process, although some aspects of it require close human scrutiny.[135] Shifting to a personalized regime would further stretch the rather thin enforcement effort beyond its feasible limits. Furthermore, personalization

131. *See generally* Ariel Porat & Lior J. Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417 (2014). *See also* Arbel & Becher, *supra* note 77, at 26.

132. *See* Arbel & Becher, *supra* note 77, at 92. *See generally* Christoph Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law*, 86 U. CHI. L. REV. 309 (2019). For a suggestion to do so, see Johansen et al., *supra* note 69, at 12–13.

133. *See* Busch, *supra* note 132, at 329–30. For a discussion of the general skepticism about personalization regarding disclosure, see BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 134.

134. The fact that personalization is carried out through an intermediation process initiated by a separate entity most likely causes the uniqueness of personalization challenges that this Essay addresses and is what distinguishes it from the various instances covered in Porat and Strahilevitz's general discussion of their model's challenges. *See* Porat and Strahilevitz, *supra* note 131.

135. *See supra* Part I.B.2.

would undermine the ability to rely on crowdsourcing initiatives to monitor proper privacy disclosures and labeling, given the splintering of the recipient audience into many subgroups. In other words, if personalized labels are distributed, the number of people with access to each specific label to enable its review and with an interest in doing so would substantially diminish, further limiting the small pool of qualified assessors. Automated measures may be considered to examine the accuracy of personalized intermediation, but as explained above, distinct human supervision is essential to supplement this process—at least until AI and machine-learning methods are good enough to engage in independent labeling and intermediation. Thus, in view of the insights provided by Reidenberg, personalized disclosures would multiply regulators' tasks, perhaps creating an overly burdensome challenge and making personalization a poor fit for smart privacy disclosures at this time.

III. THE PRACTICAL CHALLENGES OF RANKING AND GRADING IN A REPEAT GAME

As the discussion above indicates, privacy intermediation, including labeling, has existed for some time, but it has yet to be broadly and successfully implemented. The mapping and analysis above detail how labeling schemes can be designed to potentially overcome the challenges, relying on the important work of Reidenberg and others. Successfully designing and deploying labels marks only the start of an efficacious intermediation process. This initial step must be followed by an ex post examination that the firm's policy disclosures are consistent with the labels provided. This examination is best conducted by a process that combines automation, crowdsourcing, and human intervention. These steps must be followed by an enforcement process that takes measures against firms whose conduct fails to meet the standards and commitments set out in their privacy policies—long and short.[136]

Beyond these aspects of the process—and the challenges they create—lies a secondary set of problems and unintended consequences: the potential trivialization of labels and rankings over time, which undermines the very objectives that intermediation strives to promote. These must be addressed when assuming that the intermediation of privacy polices will play a meaningful role in the personal information ecosystem. Ironically, this risk becomes more acute once the labels gain importance and salience. The discussion that follows suggests that policy makers should remain vigilant even after the intermediation process has been implemented and moved to the operational stage. This is because affected parties—naturally, those being labeled and ranked—have a strong incentive to act strategically to

136. This is, to some degree, already carried out by the FTC, albeit in a limited way, given the scarcity of resources. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

improve their position. Given these concerns, unique policy responses are needed.[137]

To demonstrate and explain this concern, consider the instructive case of restaurant hygiene.[138] Several cities, such as New York City and San Diego, have introduced grading systems to signal restaurants' sanitary conditions.[139] Many are familiar with the letter-based ranking prominently displayed at establishments that serve food or have kitchens. These labeling (and thus, intermediation) initiatives were thought to enhance transparency and lower food poisoning levels throughout the regulated areas.[140] Yet, a study that tracked and assessed the effect of this regulatory scheme discovered that the overall ranking-driven improvement in hygiene was merely an illusion.[141] The study also found the grading processes to be deeply flawed, with a clear bias toward higher grades.[142] The hygiene grading process, therefore, produced substantial grade inflation. Although establishments with low grades became scarce, the overall health benefit was questionable. Seeking explanations for the rankings' failure to promote hygiene, the study dug deeper, exposing systematic failings in the ranking process. It found that, given the visibility of the hygiene intermediation scheme, when establishments received a low grade, they sought to appeal the process; this granted them the right to a reinspection, for which they were often able to prepare.[143] The motivations for requesting a reinspection may have also been linked to the fact that grading turned out to be a difficult task, with vast disparities between the grades given by different inspectors at different times.[144]

The vast wave of reinspection of restaurant hygiene had several unfortunate outcomes. First, it resulted in an inefficient allocation of resources. Rather than cracking down and sanctioning establishments with very poor hygiene,[145] ranking institutions invested substantial resources in the reinspection of clean establishments that missed an "A" grade by a few points.[146] Furthermore, the reinspection process was often prearranged, limiting the effects of a surprise visit (an aspect that might have less of an effect on the privacy issue explored here, as I discuss below).

Returning to the matter of privacy disclosure, it is reasonable to consider the lessons that may be learned from this ranking blunder and the biased

137. For an exploration of the challenges arising from the ongoing adjustments of behavior in the algorithmic space, see generally Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1 (2018).

138. *See generally* Daniel E. Ho, *Fudging the Nudge: Information Disclosure and Restaurant Grading*, 122 YALE L.J. 574 (2012).

139. *See id.* at 583–85 (listing jurisdictions).

140. *See id.* at 582–83.

141. *See* BEN-SHAHAR & SCHNEIDER, *supra* note 15, at 43.

142. In San Diego, 99.9 percent of the establishments received a maximum grade. *See* Ho, *supra* note 138, at 610.

143. *See id.* at 612 (noting the limited value of "strategic cleanups for regrading").

144. *See id.* at 642.

145. *See id.* at 647.

146. *See id.*

grades that ensued. Thus we must ask: would the privacy-related labeling system lead to grade inflation and the trivialization of the results over time? To learn from the restaurant hygiene case, we must look beyond its raw facts. The hygiene study focuses on two possible sets of problems that would most likely plague privacy intermediation should it gain traction and importance. The first pertains to the *process* (of repeated, wasteful retesting) and, second, with its *outcomes* (the grade inflation and limited attention paid to institutions with poor hygiene). Below, I consider both elements from the perspective of privacy.

Regarding the *process*, it is fair to assume that, with a widespread, government-initiated, and broadly recognized labeling scheme, relatively low grades (even those merely falling from a maximum one) would prove harmful to a firm's reputation. Therefore, grading will be followed by grading disputes. This prediction is not far-fetched even if we move beyond the realm of hygiene and into that of technology. For years, e-commerce firms, such as eBay, have been devoting substantial resources to resolving disputes concerning reputation resulting from contested grades.[147] As reputation gained prominence in the digital age, the grading dynamics it featured have become vitally important to those subjected to it.[148] The same dynamic might follow regarding privacy-related grades, which will gain importance over time. With such importance emerging, pressure to receive a higher grade will follow. Such pressure serves not only as an incentive for parties to work harder to improve the evaluated process but also to attempt to influence the grading process. Therefore, it is fair to assume that if privacy labeling and grading become important, privacy grading disputes will tax and encumber the intermediation process. Unchecked, the disputes that will follow can lead to the allocation of funds to reinspect entities that are relatively privacy-abiding, rather than investigating egregious privacy violations—given that funding for these intermediation objectives is limited.

Privacy ranking and restaurant sanitation are indeed very different topics, and one might question the applicability of lessons from one to the other. But given the nature of the difference between them, such differences arguably exacerbate the problems that might evolve in the privacy realm, thus strengthening the need to closely monitor the problem here addressed in the privacy context. Indeed, there are many more accessible websites and data-collecting entities than kitchen facilities in any given city, county, or state. Furthermore, food poisoning is assumedly far more noticeable than breaches of privacy. As opposed to the inspection of food establishments, privacy inspections will, most likely, be carried out by private parties in a diffused process. In view of all these differences, it is fair to assume that, with respect to privacy, inspection resources would be even more limited and further stretched by reinspection than they have been for food inspection. Furthermore, the absence of government inspection will lead to an even

147. *See* M. ETHAN KATSH & ORNA RABINOVICH-EINY, DIGITAL JUSTICE: TECHNOLOGY AND THE INTERNET OF DISPUTES 70 (2017).

148. *See* COHEN, *supra* note 21, at 79–80.

greater disparity in testing results, given higher turnover of inspectors who will not have the job security that government positions offer. Similarly, disparities in the review of privacy policies will be greater than those in sanitation, in view of the inherent ambiguity of privacy as opposed to the relatively concrete issues involved in sanitation. Finally, because the stakes of privacy ranking are lower than those involved in sanitation (where food poisoning can cause bodily damage), the inspectors will be likely to take their job less seriously, opening the door to errors. The prospect of errors and the reversal of a decision in response to appeal will eventually lead to higher demand for reinspection, resulting, again, in poor resource allocation for inspections. This all might change with a shift to a wholly automated process premised on AI, which might lead to fewer errors and limited discrepancies between reviews. Yet, as explained above, this is not yet the case, and until technology catches up, appeals are going to be a substantial part of the assessment process.

The prospects of disputes and the reexamination that might follow will also affect *outcomes*. Ongoing requests to review the ranking in a complicated process that leads to disparate results may end up pushing grades upward. Only low grades would be appealed, as website operators try their luck with a fickle grading process. Given the competition between labeling entities, entities that receive a low ranking (or a "bad" label) might trade one intermediary for another that is more likely to grant a better review. This dynamic will initiate a "race to the top" in grades (or "to the bottom" in grade validity). Therefore, it is quite likely that the grading and labeling schemes will lead to grade inflation, creating a somewhat meaningless environment in which a vast number of entities receive maximum grades that do not necessarily reflect a high level of privacy.

A caveat is in order here. Unlike the case of hygiene, knowledge of an upcoming privacy inspection need not lead to biased results. Privacy policies, unlike kitchens, cannot be hastily cleaned and subsequently neglected. Admittedly, a privacy policy could be changed only during the inspection period, then changed back after its conclusion. But, such actions would likely amount to fraud and thus are less likely to occur (and they are beyond the scope of this analysis). Therefore, it is difficult to affirm with confidence that substantial grade inflation will follow repeated privacy inspections, but the elements noted above do convincingly seem to point in that direction.

The potential problems related to the process and outcome of labeling are not beyond repair and must be addressed through various structural measures taken when the systems are being introduced. Below are several suggestions that may be further developed. First, grade inflation can be addressed by applying and enforcing grading curves or stricter grading measures.[149]

149. Applying grading curves might raise fairness problems as it might result in situations in which small differences between entities might be nonetheless reflected in large ones in the ranking process, given their position on the curve. For a discussion of these issues and their normative implications, see Jane R. Bambauer et al., *When a Small Change Makes a Big*

Second, overwhelming requests for reinspection and challenging of grades must be regulated as part of system design by limiting the right of appeal and flagging cases where there is a substantial grade disparity at reinspection.

Third, responses to both concerns of process and outcome should be through various forms of transparency.[150] For example, when ranking by third parties is made publicly available, it must be supplemented by information about reexaminations, grade distribution, and errors revealed during reinspection. Although the public will most likely ignore or fail to properly comprehend such metatransparency data, the prospect of its disclosure is likely to mitigate concerns of resource misallocation and grade inflation. As in other domains, the "spotlight bias" suggests that the prospect of these forms of information disclosure will influence and improve the way providers operate ex ante—after all, executives do not like to disclose that they are running a biased operation.[151] Furthermore, apparent failures in the grading process and grading outcomes should provide an incentive to those involved in these processes to either correct the grades or risk losing credibility (or government licensing, when applicable). This would be especially true when some form of competition between labeling entities exists.

Finally, it is fair to assume that entities that are ranked or labeled in a way they disagree with may seek legal remedies. Thus, engaging in intermediation—or failure to do so properly—may result in legal liability for the ranking entity, whether it is the government, a trusted NGO, or a for-profit corporation. Generally, policy makers would be wise to strive to ensure that such liability is properly balanced and does not lead to overdeterrence by those claiming to have been wronged (by bringing legal action and claiming damages). Yet they might also use the prospect of such liability to resolve some of the noted concerns. Among others, legislatures could limit, and thereby calibrate, such liability by introducing laws shielding designated ranking entities from liability when it is proven that they carried out their task diligently. Such a legal regime may resemble the way in which the Fair Credit Reporting Act[152] (FCRA) preempts most common-law and state law claims by ranked individuals against credit rating agencies, if the agencies are found to comply with certain rules and standards.[153] In addition to such laws (and clearly in their absence), labeling and ranking providers should be allowed to employ other strategies as a hedge against such risks;

Difference, U.C. DAVIS L. REV. (forthcoming 2022). Generally, if the rules of ranking are known in advance to all relevant parties, the risk of unfairness is somewhat mitigated. *See id.*

150. *See* Ho, *supra* note 138, at 650; *see also* Waldman, *supra* note 2, at 177–78 (discussing the importance of maintaining transparency in design).

151. *See* George Loewenstein et al., *Disclosure: Psychology Changes Everything*, 6 ANN. REV. ECON. 391, 403 (2014).

152. Pub. L. No. 90-321, 82 Stat. 146 (1968) (codified as amended in scattered sections of 15 and 18 U.S.C.).

153. *See* Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 4–14 (2008) (providing a critical discussion of the various steps the U.S. Congress has taken to limit the liability of credit agencies by shielding them from state law claims and allowing claims under the FCRA to continue, but only if certain conditions are met).

for example, by insuring their activities or engaging in other risk-spreading strategies.[154]

Further consideration of these aspects of intermediary liability and its limits is an integral part of any attempt to design an efficient labeling scheme. Such moves are closely related to the process- and outcome-based concerns discussed here. Indeed, liability issues must be tied to the various institutional decisions contemplated above, regarding the precision of the process, the grading range, and the extent of appeals—for example, by providing regulatory liability waivers only to ranking entities that meet an acceptable standard of conduct.[155] Thus, in addition to the requirement for transparency, the government may use liability as a lever to mitigate the risk of ranking trivialization over time.

CONCLUSION: LONG LIVE THE PRIVACY POLICY!

The insights that Reidenberg, a serious and seasoned privacy scholar, derived from his studies led him to a conclusion that many in the privacy community would prefer to ignore: the privacy policy is here to stay. These policies are the go-to documents that consumers, experts, journalists, judges, and apparently academics examine to assess privacy practices. Like many other legal documents, privacy policies are rarely read, but they have unique qualities that Reidenberg went to great lengths to expose and explore. They cannot be easily grouped with terms of service, terms of use, and other standard form contracts.

With some tweaking, Reidenberg's work could certainly be used to establish a strategy as to how to educate the public about the content of these policies. Such education would entail smart design of intermediation and an ongoing evaluation process. This Essay mapped out some of the important steps a sustainable labeling process should include. It also pointed out the need to establish and prioritize the objectives of labels, set aside personalization efforts, and attend to a structured appeals process.

My work on this Essay started out as a celebration of Joel Reidenberg's scholarship. After completing its first draft, I received the terrible news of Joel's passing. The recognition that Joel will not read these words and build on them in his future projects is greatly saddening. That said, I hope that others will continue walking in his large footsteps and address the crucial matters he pursued with the same rigor, passion, and gravity that characterized Joel's long and fruitful career. He will be missed, and may his memory be a blessing.

154. One of these could be self-insurance by charging a premium from all consumers.

155. For a passing reference to the liability issue in ranking, see generally Kamara and De Hert, *supra* note 28.