MOVING BEYOND THE DEVIL YOU KNOW: THE NEED FOR SUBSTANTIVE REGULATION OF ALGORITHMIC DECISION-MAKING SYSTEMS

Harsimar Dhanoa*

CITE AS: 5 GEO. L. TECH. REV. 125 (2021)

TABLE OF CONTENTS

I. INTRODUCTION

The willingness to be exposed to risk—to trust another—enables individuals to cooperate and accomplish more together than what would be possible individually.[1] The impacts of this trust resonate throughout society even if they are not outwardly obvious:

* Associate, Hogan Lovells US LLP. Georgetown University Law Center, J.D 2020; University of California, Los Angeles, B.A. 2015. I would like to thank Professors Anupam Chander and Greg Scopino for their encouragement and thoughtful feedback as well as to Georgetown Law's Institute for Technology Law & Policy for hosting the Georgetown Law Technology Review Student Writing Competition. I am also especially grateful to the editorial team of the Georgetown Law Technology Review for their invaluable assistance and incredible hard work.

> We trust that architects and builders have created bridges that will support us when we cross them. We trust that merchants will accept the small, green pieces of paper (or digital code) we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest, and we trust that our friends will support us and look out for us. *Without trust, our modern systems of government, commerce, and society itself would crumble.*[2]

The pursuit of fostering this trust is not static. As modern interconnectivity becomes increasingly digital, entities ranging from local grocery stores to world governments collect, store, and use information about us.[3] In turn, regulatory efforts have focused on promoting trust in these information-based relationships.[4] In the context of privacy and data security, the Fair Information Practice Principles, developed by the U.S. federal government in the 1970s, provided a theoretical base for trust-promoting regulations applicable to information relationships between consumers and data collectors.[5] In practice, this framework fell short when regulators adopted transparency as the primary mechanism for trust, with enforcement being limited to circumstances where companies misrepresented their privacy practices.[6] In relying on transparency, the framework favors allowing individuals to interact with the devils they knew rather than those they didn't. However, this approach ignores the existing power dynamic underlying modern information relationships, undermining their efficacy. This, in turn, accelerates the erosion of trust

---

[1] *See generally* SHELLEY E. TAYLOR, THE TENDING INSTINCT: WOMEN, MEN, AND THE BIOLOGY OF OUR RELATIONSHIPS 39 (2014) ("Indeed, the ability to cooperate and to promote social harmony have clear social advantages. You are more likely to survive to reproductive age if you avert war, for example, than if you win it.").

[2] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 433 (2016) (emphasis added).

[3] *Id.*

[4] *See, e.g.*, Commission Regulation 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter GDPR].

[5] *See generally* Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM (Jan. 4, 2008), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ [https://perma.cc/6MUN-EGXS] (describing the origins of the Fair Information Practice Principles).

[6] *See generally* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, 7–10 (1998), https:// www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/A7MR-WVDL] (identifying "five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress").

between consumers and business entities that collect, use, and store their personal information.

Now, as these entities turn to algorithmic systems to draw non-intuitive inferences about individuals' behaviors and preferences from this personal information, the differences in the power dynamics between individuals and entities using these systems are increasing. While algorithmic decision-making systems import the need for trust underlying all information relationships, they further require trust not only in the entity using the system, but in the systems themselves. As regulators seek to promote trust in the adoption of algorithmic tools, these efforts must focus on more than transparency alone.[7] Instead, global economies seeking to regulate algorithmic systems should foster consumer trust in these systems by imposing substantive regulations that supplement and reinforce transparency. Adopting these regulations would both improve consumers' assessments of the trustworthiness of algorithmic decision-making systems and the companies that use them and decrease the amount of trust needed for consumers to be willing to provide their personal information for these tools.

Part II discusses the importance of trust in fostering commercial transactions, first using Roger Mayer's tripartite model of trust to evaluate trust-promoting frameworks before turning to contract law as a formalized effort to foster trust. Part III analyzes trust in the privacy and data security context, highlighting the focus on transparency as a sole basis of trust and discussing why this approach has often failed. Part IV discusses the search for trust in the modern algorithmic age, noting that while there is some convergence around robust modalities of trust, many existing legal approaches to algorithmic accountability focus again on transparency alone. In light of this issue, Part V recommends that governments implement substantive regulation, backed with powerful enforcement, to foster consumer trust in algorithmic systems.

II. THE ROLE OF TRUST IN FOSTERING COMMERCIAL TRANSACTIONS

Virtually every commercial transaction conducted over time carries risk and, in turn, relies on trust.[8] Trust theorist Roger Mayer's seminal work on trust as the willingness to take risk uses a tripartite model of trust that helps to demonstrate its contours.[9] Contract law illustrates the application of Mayer's model of trust to the formalized pursuit of fostering trust and commercial transactions between strangers.

---

[7] *See infra* Part V.

[8] *See* Kenneth J. Arrow, *Gifts and Exchanges*, 1 PHIL. & PUB. AFF. 343, 357 (1972).

[9] *See generally* Roger C. Mayer, James H. Davis & F. David Shoorman, *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709 (1995).

While scholars across a variety of academic disciplines have written on trust, the definition of trust employed by most scholars is the willingness of one party, the trustor, to make itself vulnerable to another, the trustee.[10] Such trust exists along two dimensions. The first reflects the quantity of trust with a continuum of untrustworthiness on one end and trustworthiness on the other. The second, in contrast, reflects not all trust is equal, and reflects the justification for this trust with affective trust on one end and cognitive trust on the other.[11] Affective trust is emotional in nature and is based upon shared experiences, histories, or values.[12] This trust develops over time as parties demonstrate their trustworthiness to each other, and this is often what individuals envision when they think of trust.[13] Conversely, cognitive trust represents a cost-benefit analysis in which the willingness to take risk is the result of balancing the potential benefits of exposing oneself to risk against the potential costs of that risk.[14] While interactions between strangers may lack affective trust, cognitive trust can provide the basis for successful commercial transactions between these individuals.

Mayer's model of trust describes three interrelated factors that impact the decision to trust: ability, integrity, and benevolence. First, "ability" refers to having the knowledge, skills, or competencies that allow a trustee to have influence over the trustor within a particular domain.[15] This factor reflects that the decision to trust depends on the convergence between the circumstances in which the trustor decides to trust and the trustee's ability in those circumstances.[16] Second, "integrity" refers to the perception that the trustee adheres to a set of principles the trustor finds acceptable.[17] This factor is influenced by the consistency of the trustee's past actions, credible communications about the trustee from other parties, and the extent to which the trustee's actions are congruent with their words.[18] Third, "benevolence"

---

[10] *See* Claire A. Hill & Erin Ann O'Hara, *A Cognitive Theory of Trust*, 84 WASH. U. L. REV. 1717, 1723–24 (2006) ("[T]rust is a state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster."); *id.* at 711 (defining trustor and trustee).

[11] Ronald J. Colombo, *The Role of Trust in Financial Regulation*, 55 VILL. L. REV. 577, 580 (2010).

[12] Frank B. Cross, *Law and Trust*, 93 GEO. L. J. 1457, 1464 (2005).

[13] *See* Oliver E. Williamson, *Calculativeness, Trust, and Economic Organization*, 36 J. L. & ECON. 453, 479, 482–84 (1993) (referring to affective trust as "personal trust").

[14] Cross, *supra* note 12, at 1465.

[15] Mayer, Davis & Shoorman, *supra* note 9, at 717–18.

[16] *Id.* at 717. For example, while an experienced attorney may appear more worthy of trust when seeking legal advice, their ability in the legal field would not necessarily merit trust in other domains, such as medicine.

[17] *Id.* at 719–20.

[18] *Id.* at 719.

refers to the extent to which the trustor believes that the trustee has its interests in mind as opposed to operating solely out of an egocentric profit motive.[19]

While there is a high level of trust when each factor is present to a large degree, meaningful amounts of trust can still develop when each factor is present to a lesser degree. Thus, the efficacy of a trust-promoting mechanism can be evaluated by assessing its impact on these factors.

Contract law is likely the clearest illustration of trust-promoting mechanisms in action. Because parties typically lack sufficient information about each other to develop independent assessments of trustworthiness, contract law serves as a trust-promoting mechanism that allows parties to more confidently engage in economic activity without the affective trust that otherwise exists in their close, personal relationships.[20] By creating default rules to resolve certain discrepancies and encourage negotiation, and by creating mandatory rules to discourage certain conduct, contract law reduces both the transaction costs associated with investigating whether the other party is trustworthy and the amount of trust needed for the transaction.

To this end, contract law embodies the factors described in Mayer's model of trust. When courts enforce parties' promises, the potential for remedies following a breach of contract lowers the amount of trust necessary for unacquainted parties to engage in the transaction.[21] Additionally, the duty of good faith applied by American courts indirectly increases benevolence by minimizing malfeasance or other opportunistic behaviors.[22] In some extreme contexts, courts have morphed the duty of good faith into a fiduciary duty outside of the contract.[23] Last, contract law indirectly impacts ability as a factor of trustworthiness by allowing parties to stipulate the amounts and types of risk in their transaction structure.[24] Where ability is lacking, contractual provisions can lower the amount of trust needed and offset the risk of such a low-trust transaction with provisions for liquidated damages. While this damages provision does not increase the counterparty's ability to perform on time. it lowers the level of trust needed for the parties to enter into the agreement and incentivizes timely performance. Similarly, situations where a party has the ability to perform according to the terms of their agreement but chooses not to do so reflect a lack of integrity. The availability of breach-of-contract claims and remedies recognizes and compensates the party for this

[19] *Id.* at 718–19.
[20] Raymond H. Brescia, *Trust in the Shadows: Law, Behavior, and Financial Re-Regulation*, 57 BUFF. L. REV 1361, 1402 (2009).
[21] *See* Erin O'Hara, *Trustworthiness and Contract*, *in* MORAL MARKETS: THE CRITICAL ROLE OF VALUES IN THE ECONOMY 4 (2007).
[22] *See id.*
[23] *See id.*
[24] *See id.*

lack of trust, enabling transactions that otherwise would not happen to proceed.

III. THE PURSUIT OF TRUST IN THE INFORMATION AGE

Though largely underexamined in legal scholarship, Professors Neil Richards and Woodrow Hartzog suggest that trust is important in privacy disputes; they argue that trust is the "glue that holds together virtually every information relationship" because the disclosure of personal information leaves the discloser more vulnerable than before.[25] This vulnerability is central to the Fair Information Practice Principles (FIPPs), a set of principles established in the early 1970s that lays out the normative view of how data privacy should be protected.[26] In the nearly fifty years since their first publication, a variety of government and inter-governmental agencies have expanded on the FIPPs to create a canon of fair information principles.[27] However, despite the importance of trust in the privacy context, the effectiveness of the FIPPs was severely undermined when the only mechanism to protect this trust became transparency.

A. Privacy and Trust

Derived from a 1973 report from the Department of Housing, Education, and Welfare (HEW), the FIPPs grew out of concerns about the increasing use of computerized databases and the further attenuation between the data subject and the entity maintaining the database.[28] The HEW Advisory Committee recommended that Congress adopt five principles that made up a "Code of Fair Information Practices":

> (1) There must be no personal data record-keeping systems whose very existence is secret.
> (2) There must be a way for an individual to find out what information about him is in a record and how it is used.

---

[25] *See* Richards & Hartzog, *supra* note 2, at 449 n.65.
[26] *See* Dixon, *supra* note 5.
[27] *See, e.g.*, ORG. FOR ECON. COOPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).
[28] *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 29 (1973) ("There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers-unknown, unseen and, all too frequently, unresponsive.").

> (3) There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
> (4) There must be a way for an individual to correct or amend a record of identifiable information about him.
> (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[29]

The Mayer model of trust illustrates how the Code of Fair Information Practices principles address ability as a factor of trust. For example, under the second principle, an individual using a weather app could determine what location information the app stores and stipulate that the information be used solely for providing weather forecasts. Using the same example, the third principle would empower an individual to stop the weather app from using location information in ways that do not comply with the originally-contemplated information relationship, such as by selling location information to an unknown third party. Later expansions on these principles, such as the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, further required that entities collecting and storing personal information about individuals should be accountable for complying with privacy-protective measures.[30] In requiring accountability, the OECD Guidelines give effect to the above principles and recommend that personal information should only be obtained by lawful and fair means, increasing both integrity and benevolence as correlating to non-malfeasance.[31] In turn, this OECD approach increases individuals' trust in these systems and decreases the amount of trust needed to be willing to provide personal information.

B. Trust Promotion in the Privacy Context

In the privacy context, transparency has become the sole mechanism for trust promotion. However, in practice, this reliance on notice-and-choice is limited in its effectiveness in promoting trust. While more recent efforts at trust promotion through substantive regulation are promising, consumer trust in the digital economy has significantly eroded.

---

[29] *See id.* at 41.
[30] *See* ORG. FOR ECON. COOPERATION AND DEV., *supra* note 27.
[31] *See id.*

1. Transparency as Trust Through Notice-And-Choice

Despite the FIPP's theoretical efficacy in promoting trust and protecting privacy, its implementation, at least within the United States, has been lackluster due to the reliance on the notice-and-choice model. In a 1998 report to Congress on the state of online privacy, the Federal Trade Commission (FTC) consolidated the FIPPs into four core principles of privacy protection— "Notice," "Choice," "Access," and "Security"—with particular emphasis on the first principle.[32] Under this notice-and-choice framework, websites or online services provide notice of their information practices alongside the opportunity for the individual to either deny consent or opt out of the transaction altogether.

The adoption of notice-and-choice as a trust-promoting mechanism reflected a light-touch approach. By arming consumers with information and allowing them to make the ultimate decision about the processing of their personal information, regulators believed that consumers would be able to make "an informed decision as to whether and to what extent to disclose personal information" through a mechanism that is relatively cheap to implement for companies.[33] Further, because notice regimes opt for disclosures of conduct rather than substantive limitations of those conduct, they are thought to minimize the impact on innovation and competition.[34]

2. Limited Effectiveness of Notice-And-Choice in Practice

The reduction of the FIPPs to a notice-and-choice model severely undermines the overall promotion of trust in information relationships due to a combination of ineffective notices and the absence of meaningful choice.

a. Ineffective Notices

One of the primary critiques of the notice-and-choice model is the limited effectiveness of disclosure regimes. In discussing the limitations of notice in the context of securities regulation, Professor Susanna Kim Ripken highlights three factors that illustrate the ineffectiveness of notice alone as an instrument for promoting consumer trust: the difficulty of communicating the sheer complexity of modern business organizations in understandable disclosure documents, the use of formalized language to minimize liability

[32] FED. TRADE COMM'N, *supra* note 6.
[33] *See id.*; *see also* M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1048 (2012).
[34] M. Ryan Calo, *supra* note 33, at 1048.

rather than provide information, and the impact of cognitive and behavioral biases and constraints.[35]

First, capturing the magnitude, reach, technology, and complexity of large multi-national business organizations in a simple description within disclosure documents presents a near Sisyphean task.[36] The mass proliferation and expansion of platforms, third-party service providers, and cross-border data flows exponentially increases the complexity of the modern digital ecosystem. In the context of financial regulation, "[e]ven trained accountants are unable to determine, without detailed investigation, the intrinsic value of securities of corporations whose property and activities extend into many States and foreign countries."[37] Similarly, consumers seeking to meaningfully assess the trustworthiness underlying potential information relationships are often out of luck.

Second, notices within disclosure regimes are often drafted with formalized language meant to shield the entity from liability rather than to provide the consumer with meaningful information.[38] Within the context of privacy policies, as the instruments of notice-and-choice, this materializes through complex documents that nonetheless do not alleviate uncertainty or provide a meaningful basis for consumers to assess trustworthiness.[39] As one study highlighted, consumers would need to spend 244 hours a year to read the privacy policies that they typically encounter online.[40] Furthermore, privacy policies rely on vague language such as referring to "affiliates" or "third parties" rather than specifying parties by name, meaning that despite the length of material consumers are faced with, they are unable to fully assess the trustworthiness of the entity providing the notice.[41] Describing these notices as saying much but not saying anything at all, however, would not be an accurate description of their role. The use of circumlocution with notices provides entities with a shield against both government and private liability.

---

[35] *See* Susanna Kim Ripken, *The Dangers and Drawbacks of the Disclosure Antidote: Toward a More Substantive Approach to Securities Regulation*, 58 BAYLOR L. REV. 139, 185–88 (2006).
[36] *See id.* at 185–86.
[37] *See id.* at 186 (quoting *Federal Securities Act: Hearing on H.R. 4314 Before the H. Comm. on Interstate & Foreign Commerce*, 73rd Cong. 92 (1933), *reprinted in* 2 LEGISLATIVE HISTORY OF THE SECURITIES ACT OF 1933 AND SECURITIES EXCHANGE ACT OF 1934 (J.S. Ellenberger & Ellen P. Mahar eds., 1973).
[38] *See id.*
[39] *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 617, 620 (2018).
[40] *See id.* (citing Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543 (2008)).
[41] *See id.* at 617.

In the context of government liability, the FTC has stepped into the role of de facto privacy regulation since the late 1990s, using its authority under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[42] However, absent some other specific statutory grant of authority, the FTC's enforcement ability has been limited to enforcing the promises made by companies to their consumers through their privacy policies, thus focusing on the substantive disclosures.[43] This "broken promise" privacy jurisprudence is often based on explicit promises included in a company's privacy policy,[44] such as promises to maintain confidentiality or to refrain from disclosing information to third parties,[45] though the FTC has also looked to implied promises suggested elsewhere on the website or online service. While states have been more willing and able to address consumer privacy concerns in the absence of comprehensive legislation at the federal level, they too often approach privacy protection through the use of state prohibitions on unfair or deceptive acts and practices. For example, the laws of Nebraska, Oregon, and Pennsylvania specifically address false or misleading statements within privacy policies.[46] Thus, the use of ambiguous or sufficiently cautionary language allows entities to claim that they are better informing consumers, while instead working to "reduce the risk of liability for omitting a material fact or disclosing a 'half truth.'"[47]

Such disclosures also provide a shield from private liability through the basis of consent. In these instances, a company's privacy policy or terms of service function not only to inform the user of the company's information practices, but also to do so in a way that limits users' abilities to pursue litigation against behavior they might consider outside the proper scope of the information relationship.[48] For example, two class-action plaintiffs separately brought suits against Google and Yahoo alleging that the companies violated state and federal anti-wiretapping laws by intercepting and scanning their

---

[42] 15 U.S.C. § 45 (2012).

[43] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004).

[44] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 629–30 (2014).

[45] *See, e.g.*, Complaint, *In re* Eli Lilly & Co., 133 F.T.C. 763 (2002).

[46] *See, e.g.*, NEB. REV. STAT. § 87-302(a)(14) (2020); OR. REV. STAT. § 646.607 (2020); 18 PA. CONS. STAT. § 4107(a)(10) (2020).

[47] *See* Ripken, *supra* note 35, at 186 n.181 (quoting Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 WASH. U. L. Q. 417, 429 n.58 (2003)).

[48] *See, e.g.*, Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint, *In re* Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767 (N.D. Cal. 2019) (No. 18-MD-02843-VC); *In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016 (N.D. Cal. 2014); *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784 (N.D. Cal. Sept. 26, 2013).

respective users' incoming and outgoing emails for content.[49] In both suits, the companies argued for dismissal, with differing levels of success, on the basis that the Wiretap Act was not violated because users expressly consented to the interception of their emails.[50]

More recently, this strategy was also attempted in the wake of the Cambridge Analytica scandal, in which Cambridge Analytica used the personal information of millions of Facebook users to send targeted political messages during the 2016 presidential campaign.[51] Here, Facebook unsuccessfully sought to dismiss litigation alleging that it compromised users' personal information, arguing instead that "Facebook users consented, in fine print, to the wide dissemination of their sensitive information."[52] These three instances illustrate that while the notice-and-choice model envisions disclosure as a sword in the hands of consumers seeking to assess trustworthiness, companies are incentivized to draft these notices in such a way that provides them a shield from liability when they engage in conduct that undermines users' trust.

Third, while information can serve as a powerful tool, its effectiveness is constrained by the behavioral and cognitive limitations of those processing, or attempting to process, that information. Criticisms of disclosure regimes generally bemoan the whole cloth adoption of the assumptions underlying disclosure-based regimes: that people are rational and that material information given to individuals provides a rational basis for decision-making.[53] These critics note that given the high costs of acquiring perfect information, individuals' decision-making processes rely on heuristics, creating a bounded rationality; this bounded rationality, in turn, requires a reevaluation of the assumptions at the heart of the notice-and-choice model.[54] For example, when faced with too much data, individuals can become distracted by less relevant data and ignore highly relevant information.[55] Additionally, the anchoring heuristic—the tendency of individuals to latch onto or "anchor" early information as a reference for all future information—

[49] *See* Google, 2013 U.S. Dist. LEXIS 172784; Yahoo, 7 F. Supp. 3d 1016.

[50] *See* Google, 2013 U.S. Dist. LEXIS 172784, at *46–57 (rejecting Google's explicit and implicit theories of consent); Yahoo, 7 F. Supp. 3d at 1028–32 (accepting Yahoo's theory of explicit consent).

[51] *See generally* Pretrial Order No. 20, Facebook, 402 F. Supp. 3d at 776.

[52] *Id.* at 777.

[53] *See, e.g.*, Rothchild, *supra* note 39, at 614–29 (2018); Ripken, *supra* note 35, at 186.

[54] *See* Rothchild, *supra* note 39, at 619–21; *see also* Ripken, *supra* note 35, at 158 n.61 (highlighting a body of behavioral evidence demonstrating that people do not consistently act in accordance with rational choice theory).

[55] *See* Jacob Jacoby, *Perspectives on Information Overload*, 10 J. CONSUMER RES. 432, 433 (1984) (cited in Ripken, *supra* note 35, at 160 n.70).

can undermine the true effectiveness of disclosure.[56] In the context of privacy disclosures, this manifests through some consumers equating the title "privacy policy" with the belief that the entity has a "policy of privacy" and that the existence of such a document refers to specific limitations on what a company may collect or disclose.[57] The prevalence of these cognitive and behavioral limitations combined with the inherent challenge in capturing the true scope of modern business organizations and the use of formalized language to minimize both government and private liability undermines the effectiveness of the notice portion in the notice-and choice model as a trust-promoting mechanism.

b. Absence of Meaningful Choice

In addition to the issues undermining the effectiveness of notices provided to consumers, the absence of meaningful choice further undermines the trust-promoting effect of the notice-and-choice model. This absence of meaningful choice results from two factors: first, differences in bargaining power between parties in commercial information relationships due to the weight of network effects and a lack of market variability, and second, the use of dark patterns to skew consumers' decision-making.

First, parties in commercial information relationships do not share similar levels of bargaining power. In the traditional context of contracts, features like the availability of remedies for breach and the flexibility to set contract terms to structure the amount of risk decrease the amount of trust parties need to engage in these transactions.[58] However, these mechanisms malfunction in the context of notice-and-choice because they rely on the "antiquated and quaint paradigm of two merchants, vigorously dickering over all terms of a contract."[59] For example, when a company offers free services in exchange for monetizing a consumer's personal information, the misuse of that information by the company leaves no contractual damages because the consumer never paid for the service and because the privacy harms are difficult to quantify.[60] Further, the scale of modern commercial entities, which makes

---

[56] *See* Ripken, *supra* note 35, at 173–74.
[57] *See* Calo, *supra* note 33, at 1029.
[58] *See supra* Part II.
[59] Wayne R. Barnes, *Toward a Fairer Model of Consumer Assent to Standard Form Contracts: In Defense of Restatement Subsection 211(3)*, 82 WASH. L. REV. 227, 269 (2007); *see also* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1216 (1983) ("Deeply embedded within the law of contracts, viewed as private law, lies the image of individuals meeting in the marketplace …").
[60] *See generally* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 96 HASTINGS L. J. 1039, 1041, (2018) (noting that "a clear conception of these harms is essential for determining both standing and remedies" and that "an overarching issue in privacy cases is

notice difficult, necessitates terms of adhesion—standardized boilerplate terms given to consumers on a "take it or leave it" basis.[61] The use of these terms diminish consumers' ability to structure their information relationships such that their trust in the other party is sufficient to undertake the amount of risk to which they will be exposed. Instead, because of the vast reliance on adhesion contracts and to ensure market stability, commenters and courts presume the enforceability of these agreements outside of the most severe and oppressive clauses.[62]

This disparity in bargaining power results from the weight of network effects which leaves consumers with few or no alternatives and a lack of market variability in contract terms where alternatives do exist. Network effects, which occur when the value of a commodity increases with the number of its users, create a disparity in bargaining power by effectively reducing the number of available alternatives. For example, in the context of social networking services, as the number of users in one service increases, so too does the pressure to join the same service. The impact of such network effects is illustrated through nominally-competing services like Facebook and Myspace. While both services function as social networks, the scale of Facebook's userbase in comparison to Myspace's and the resulting network effects undermined the comparison of both services as "close substitutes."[63] In turn, while consumers may trust the information practices of Myspace more than Facebook, they may nonetheless join the service they trust less because the user's social connections use Facebook. Further, if a service changes its terms and thus undermines the basis for users' trust, switching services may be impractical given the time, energy, and social capital that they have already invested in the service.[64] Thus, the consumer may effectively be forced to remain with a service they do not trust.

Additionally, even where the weight of network effects does not eliminate close substitutes, the vast uniformity of terms in privacy policies

---

whether the privacy violation caused any harm . . . in both data security breach cases and privacy cases, courts have struggled to recognize [such] harm." (citation omitted)).

[61] *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1451 (7th Cir. 1996) (quoting Restatement (Second) of Contracts § 211 cmt. a (Am. Law Inst. 1981)) ("Standardization of agreements serves many of the same functions as standardization of goods and services; both are essential to a system of mass production and distribution. Scarce and costly time and skill can be devoted to a class of transactions rather than the details of individual transactions.").

[62] *See* Barnes, *supra* note 59, at 248, 264–65.

[63] *See* Sean Howell, *Big Data and Monopolization* (2018) (unpublished manuscript) ("[D]ata-driven markets tend to feature strong network effects and economies of scale, which create barriers to entry that other firms may have a hard time overcoming.") (quoted in Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J. L. & TECH. 256, 273 n.45 (2020)).

[64] Lev-Aretz & Strandburg, *supra* note 63, at 289.

undermines consumers' ability to find terms more in-line with their assessments of the trustworthiness of a particular party. One survey of the privacy policies posted on twenty-five popular commercial websites noted that almost all, if not all, of the websites used cookies to collect and store information about consumers visiting the site, collected unique identifiers attached to consumers' computing devices, allowed advertising networks to collect consumers' information, collected consumers' locations, shared consumer data with third parties to permit targeted advertising, and used consumers' data to send targeted ads for the site's products.[65]

The uniformity of this behavior demonstrates that even if alternative services were available, users would nonetheless be subject to the same terms with each service, thus removing any meaningful choice. Both this uniformity of terms and the impact of network effects shifts the bargaining power in commercial relationships such that regardless of a consumer's assessment of the trustworthiness of a company, consumers have little power to act on that assessment.

Second, the use of dark patterns enables companies to nudge consumers toward decisions they otherwise would not make absent the necessary basis of trust. Dark patterns are features of interface design crafted to trick users into doing things they might not want to do but would benefit the business in question.[66] This can be done in a variety of ways, such as by using language that is confusing to users, by switching the placement of certain functions contrary to user expectations, or by including elements meant to pressure users to rush through their choices.[67] For example, in one popup delivered by Facebook about the company's compliance with the General Data Protection Regulation (GDPR), users were presented with two buttons located at the bottom of the screen of their mobile devices.[68] The bottom button was presented in a solid blue with white text stating "Accept and Continue." The top button, however, was presented in grey text stating "Manage Data Settings" on a white background, matching the background of the overall screen and appearing to be part of the overall notice. Similar to uncomfortable benches meant to discourage loitering in public spaces,[69] such differences in color when presenting a user with notice of a company's privacy policies are

---

[65] *See* Rothchild, *supra* note 39, at 624.

[66] NORWEGIAN CONSUMER COUNCIL, DECEIVED BY DESIGN 7 (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/9SHB-4CF9].

[67] *Id.*

[68] *Id.* at 14.

[69] *See generally* GORDAN SAVICIC & SELENA SAVIC, UNPLEASANT DESIGN (2013) (exploring the phenomena of designing objects, devices and strategies to influencing behavior to the benefit of particular social groups).

hostile design features intended to encourage users to select the option most beneficial to the company. In a 2015 survey of frequently visited websites' privacy policies, only nine out of 191 policies had opt-out buttons that were readily noticeable at first glance, demonstrating that this type of diversion from privacy-preserving choices is not uncommon.[70] Similarly, Facebook designed the popup such that a consumer wishing to select the least privacy-intrusive options had to navigate a near labyrinthine set of decisions, while the options most beneficial to the company required a limited number of clicks.[71] Users that selected "Accept and Continue" were able to navigate through all of the choices in four clicks, but in turn gave Facebook the widest breadth to engage in data collection and use.[72]

Such dark patterns leverage the same cognitive limitations that make notice ineffective to nudge consumers into making decisions not necessarily aligned with their assessment of the company's trustworthiness. These dark patterns and the disparity in bargaining power undermine the choice portion of notice-and-choice; in combination with the ineffectiveness of notice, this illustrates that despite the theoretical basis of "transparency as trust," in practice, transparency alone does little to promote trust.

3. Moving Beyond Transparency as Trust

Currently, governments globally are abandoning reliance on transparency alone for substantive regulations that augment notice with consumer rights and additional responsibilities for companies entrusted with consumers' personal information. Traditionally, this approach was reserved for privacy protection in high-risk sectors, such as the health and financial sectors, or for data processing of vulnerable individuals, such as children.[73] The two most notable examples of this shift to comprehensive privacy protection are the GDPR and the California Consumer Privacy Act (CCPA).[74] The GDPR, for example, addresses in part the issue of dark patterns by listing consent as one of six bases for data processing. More specifically, the GDPR requires that consent be tailored to the data's particular purpose, subject to withdrawal at any time, informed through clear and plain language separate from other terms and conditions, and freely given through affirmative action

[70] Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 82 (2018).
[71] NORWEGIAN CONSUMER COUNCIL, *supra* note *66*, at 20.
[72] *Id.*
[73] *See generally* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2012); Gramm-Leach-Bliley Act, 15 U.S.C §§ 6801–6809 (2012); Health Information Portability and Accountability Act, P.L. No. 104-191, 110 Stat. 1938 (1996).
[74] CAL. CIV. CODE § 1798.100 *et seq* (2018); GDPR, *supra* note 4.

without the presentation of a "take it or leave it" option.[75] Further, the GDPR outright prohibits the processing of sensitive categories of information, unless the consumer gives explicit consent or the processing is subject to an exception.[76] In California, the CCPA gives consumers the right to opt out of the sale of their personal information.[77]

While these provisions afford consumers the ability to meaningfully assess whether to trust a business and tailor their behavior accordingly, these mechanisms often came after users' trust in companies had significantly eroded. Within the past few years alone, the 2017 Equifax breach impacted 148 million Americans—almost half of the population of the United States—and political consulting firm Cambridge Analytica accessed the data of 87 million Facebook users to predict and influence voters.[78] One study found that a majority of Americans felt that their personal data is now less secure, that the data collection in their online information relationships posed more risks than benefits, and that escaping these risks by not being tracked was not possible.[79] Thus, while trust-promoting mechanisms such as the GDPR and the CCPA will improve some measure of consumer trust, they face an uphill challenge of repairing trust amid growing animus toward large technology companies, more commonly known as techlash.[80]

---

[75] GDPR, *supra* note 4, at Art. 7.

[76] *See* GDPR, *supra* note 4, at Art. 9.

[77] *See* CAL. CIV. CODE § 1798.120 (2018).

[78] *See* Nadeem Badshah, *Facebook to Contact 87 Million Users Affected by Data Breach*, GUARDIAN (Apr. 8, 2018), https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach [https://perma.cc/MJT6-6DH6]; Merrit Kennedy, *Equifax Says 2.4 Million More People Were Impacted By Huge 2017 Breach*, NAT'L PUB. RADIO (Mar. 1, 2018), https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach [https://perma.cc/C6PC-GDHL].

[79] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/35DD-YDTK].

[80] *See* Evelynn Douek, *Transatlantic Techlash Continues as U.K. and U.S. Lawmakers Release Proposals for Regulation*, LAWFARE (Aug. 8, 2018), https://www.lawfareblog.com/transatlantic-techlash-continues-uk-and-us-lawmakers-release-proposals-regulation [https://perma.cc/U36K-UNUJ].

IV. THE PURSUIT OF TRUST IN THE ALGORITHMIC AGE SO FAR

As companies begin to increasingly rely on algorithmic decision-making systems, trust-promotion is a primary concern for regulators and for consumers. These systems—computational processes that use technologies such as machine learning, statistics, artificial intelligence, or other data processing to make a decision or facilitate human decision-making—require trust not only as a specific manifestation of privacy concerns, but also as a necessary condition to functionality.[81] However, despite early proposals indicating that such trust-promotion may come in the form of substantive regulation, regulators may instead return to the light-touch approach that was a hallmark of early trust-promotion in the privacy context.

A. The Need for Trust in Algorithmic Decision-Making Systems

The role of trust in algorithmic decision-making systems and their use by companies both mirrors and extends beyond the role of trust in the privacy context. Just as the disclosure of personal information leaves an individual more vulnerable than before, the use of algorithmic decision-making systems magnifies this vulnerability by requiring consumers to trust both the companies that seek to use this personal information—those behind the metaphorical algorithmic "machine"—and the systems used to process that information—the "machine" itself.

First, algorithmic decision-making systems require consumers to trust in those behind the machine. As a specific use case of individual data, the use of these systems imports the need for trust that exists within any information relationship. Further, as viewed through the Mayer tripartite model, the use of algorithmic decision-making systems still implicates concerns such as whether personal information will only be used for the specific reason for which it was provided or whether companies will use personal information only in the ways that they disclose.[82] Further, the advantages of algorithmic decision-making systems to corporations are magnified through economies of scale.[83] By taking advantage of increases in the volume of data available for processing, the velocity of data generation and processing, and the multiplicity of data streams ranging from mobile devices to Internet of Things devices, these economies

[81] *See* Mind Your Own Business Act of 2019, S. 2637, 116th Cong. § 2 (defining "automated decision system") (2019).
[82] *See supra* Part III.A.
[83] *See* Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339, 352–55 (2017).

of scale are virtually unlimited.[84] The use of algorithmic decision-making systems cannot rely on the same instruments of trust-promotion in the privacy context because the advantages they provide companies further skew the power balance between these companies and consumers.

Additionally, the use of algorithmic decision-making systems implicates the need for trust in the "machine" itself. The introduction of this element in the overall information relationship raises questions categorizable by the Mayer model. First, in terms of ability, can these systems actually perform the tasks for which they are used? One clear example of where this question is raised is the well-documented failure of facial recognition algorithms when attempting to recognize people with darker skin.[85] Similarly, the use of algorithmic decision-making systems challenges assessments of integrity due to opacity in understanding how the system reached a particular decision.[86] As the dimensionality of the system's decision-making increases, its nebulousness limits the ability to assess the "integrity" of the system.[87] Lastly, the use of algorithmic decision-making systems raises questions of unintended negative consequences as byproducts of otherwise benevolent goals. For example, one study of commercial-prediction algorithms used in the health sector to identify and help patients with complex health needs discovered that the algorithms were trained to predict healthcare costs rather than illness.[88] However, by using cost as a proxy to assess which patients had complex health needs, systemic racial biases do not account for differences in access to care, and thus money spent on that care, between Black and white patients.[89] In total, the need for trust in the algorithmic age has roots in the need for trust in the information age generally, but is marked by unique dimensions that require a tailored response.

---

[84] *See id.* at 346–47.

[85] *See* Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (Aug. 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/Z5FR-F3UK].

[86] *See generally* Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889 (2018), https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf [https://perma.cc/W7AC-VGK7].

[87] *See id.* at 897–906.

[88] *See generally* Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCIENCE 447 (2019), https://science.sciencemag.org/content/366/6464/447 [https://perma.cc/RKE9-CY3Q].

[89] *See id.* at 449.

B. Past as Prologue? Current Approaches to Trust-Promotion

Given the need for both trust in the machine and trust in those behind the machine, regulators have turned to the task of trust-promotion with haste, largely through normative guidelines, and most often as non-binding recommendations. In doing so, countries appear to be following in the footsteps of the light-handed approach used in the privacy context.

As use of algorithmic decision-making systems increases, national and international organizations have begun to address the principles and values that guide the development and use of these systems. Over the past five years, more than 160 sets of normative guidelines have been released, including those by the High-Level Expert Group on Artificial Intelligence appointed by the European Commission, the expert group on AI in Society of OECD, the Advisory Council on the Ethical Use of Artificial Intelligence and Data in Singapore, and the select committee on Artificial Intelligence of the United Kingdom (UK) House of Lords.[90]

These groups focus primarily on "ethical" or "trustworthy" artificial intelligence and coalesce around five ethical principles: transparency, justice and fairness, non-maleficence, responsibility, and privacy.[91] For example, the High-Level Expert Group on Artificial Intelligence lists seven requirements for trustworthy algorithmic decision-making systems: Human agency and oversight; Technical robustness and safety; Privacy and data governance; Transparency; Diversity, non-discrimination and fairness; Societal and environmental well-being; and Accountability.[92] These principles correlate to the factors in the Mayer model of trust both directly—such as justice and fairness as a mechanism affecting integrity and non-maleficence affecting benevolence—as well as indirectly, through transparency.[93]

Despite their breadth, the thrust of these frameworks may be consolidated into transparency as trust, just as in the privacy context. First, although the convergence of these frameworks appears to indicate a unified global approach to regulating algorithmic decision-making systems, these frameworks also demonstrate substantive divergence in how these principles are interpreted, why they are important, to what issues, domains, or actors they

---

[90] *See generally AI Ethics Guidelines Global Inventory*, ALGORITHM WATCH (Apr. 2020), https://inventory.algorithmwatch.org/ [https://perma.cc/GDV9-CDAY].

[91] *See* Anna Jobin et al., *Artificial Intelligence: The Global Landscape of Ethics Guidelines*, 1 NATURE MACHINE INTELLIGENCE 389, 391 (2019), http://ecocritique.free.fr/jobin2019.pdf [https://perma.cc/EHY7-2ES6].

[92] *See* HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, ETHICS GUIDELINES FOR TRUSTWORTHY AI, 2, 14 (2019), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [https://perma.cc/S7VY-979N].

[93] *See supra* Part II.

pertain, and how they should be implemented.[94] Given this lack of true global cohesion, regulators may once again opt for the light-handed approach to quell fears of stifling domestic innovation.

Further, some critics view the development of ethics guidelines as an effort to co-opt ethics for preempting and preventing legislation.[95] As one scholar described the phenomenon: "The word ethics is under siege in technology policy. Weaponized in support of deregulation, self-regulation or hands-off governance, 'ethics' is increasingly identified with technology companies' self-regulatory efforts and with shallow appearances of ethical behavior."[96] If allowed to proceed unchecked, this "ethics washing" would subject algorithmic decision-making systems to light-touch treatment, again leading regulators to fall back on the existing mechanism available for trust-promotion: transparency.

This can most clearly be seen in the Federal Trade Commission's recent guidance on the use of algorithmic decision-making systems. While the Commission touts its experience bringing "many cases alleging violations of the laws we enforce involving AI and automated decision-making," much of the agency's guidance focuses on transparency.[97] The agency's substantive recommendations focus exclusively on the role of algorithmic decision-making systems in credit allocation through the application of the Equal Credit Opportunity Act and the Fair Credit Reporting Act, the latter of which is limited to consumer reporting agencies and companies that provide them with personal information.[98] However, the use of algorithmic decision-making systems in credit allocation has led to questions about their fairness, with critics noting that embedded biases and poor proxy choice may discriminatorily impact women and minorities.[99]

Additionally, proposed measures for trust-promotion with algorithmic decision-making systems mirror the failings of trust-promotion approaches

---

[94] *See* Jobin et al., *supra* note 89, at 396.

[95] *See generally* Ben Wagner, *Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping, in* BEING PROFILING: COGITAS ERGO SUM (Mireille Hildebrandt & Serge Gutwirth. eds. 2018), https://www.jstor.org/stable/pdf/j.ctvhrd092.18.pdf?refreqid=excelsior%3A8ec0d32a4d8e6b239444bdc4eac9a041 [https://perma.cc/M6JG-MC43].

[96] Elettra Bietti, *From Ethics Washing to Ethics Bashing: A View on Tech Ethics from Within Moral Philosophy*, PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 210, 210 (2020).

[97] *See* Andrew Smith, FED. TRADE COMM'N: BUS. BLOG, *Using Artificial Intelligence and Algorithms* (Apr. 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms [https://perma.cc/8794-UXRR].

[98] *See id.*; *see also* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2020).

[99] *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10–16 (2014).

within the privacy context. For example, the Office of Management and Budget released a draft memorandum instructing federal agencies to "avoid a precautionary approach that holds AI systems to such an impossibly high standard that society cannot enjoy their benefits."[100] Such a stance lends itself to a light-touch approach that some have characterized as "permissionless innovation."[101] Where legislative responses have been introduced, there is again a focus on half-hearted transparency efforts through algorithmic impact assessments that organizations are not required to publish.[102] Lastly, though the European Commission initially considered a moratorium on the use of algorithmic decision-making systems for facial recognition, the body ultimately reversed, instead focusing on "high-risk" applications.[103] These approaches mirror the early trust-promoting mechanisms used in the privacy context and suggest that the past may indeed serve as prologue. Despite no longer relying solely on transparency as trust in the privacy context, regulators appear to be doing just that for algorithmic decision-making systems. While regulators invoke the idea of trust, they seem to favor unrestrained innovation over true trust-promotion, perhaps lending credibility to critics who characterized this as "ethics washing."

V. RECOMMENDATIONS

Rather than wait until transparency as trust fails in the context of algorithmic decision-making systems as it did in the privacy context, regulators should focus on augmenting transparency with substantive protections effectuated through powerful enforcement. Such substantive rules could foster conduct that improves consumers' perceptions of the trustworthiness of algorithmic decision-making systems and the companies that use them. Ultimately, these regulations would result in increased

---

[100] *See* Draft Memorandum from Russell Voight, Acting Dir., Off. of Mgmt. and Budget, on Guidance for Regulation of Artificial Intelligence Applications to the Heads of Executive Departments and Agencies (Jan. 13, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf [https://perma.cc/GEK7-D8KV].

[101] *See* Abigail Slater, *Will the White House's AI Policies Lead to Permissionless Innovation?*, REG. REV. (Feb. 4, 2020), https://www.theregreview.org/2020/02/04/slater-white-house-ai-policies-permissionless-innovation/ [https://perma.cc/X5WZ-NN5N].

[102] *See, e.g.*, Federal Algorithmic Accountability Act, H.R. 2231, 116th Cong. § 3(b)(2) (2019); New Jersey Algorithmic Accountability Act, N.J. A5430, § 3(c) (N.J. 2019).

[103] *See* Elena Sánchez Nicolás, *EU Backtracks on Plans to Ban Facial Recognition*, EUOBSERVER (Feb. 20, 2020), https://euobserver.com/science/147500 [https://perma.cc/E4HB-G6H8]; *see also Commission White Paper on Artificial Intelligence: A European approach to excellence and trust*, at 17, BRUSSELS COM (2020) 65 FINAL (Feb. 2, 2020).

willingness for consumers to enter their personal information into these systems.

Although specific regulations would likely vary depending on the application of the algorithmic decision-making system, regulators should consider substantive restraints such as use limitations, non-discrimination provisions for consumers who do not want their personal information processed by these systems, and more. The important principle behind these substantive regulations is that companies seeking to use algorithmic decision-making systems would be required to obey them, regardless of whether their conduct is disclosed to the consumer.[104] Even where conduct is disclosed, substantive provisions can require specific information or formatting to refocus the purpose of the disclosure on informing consumers instead of on limiting companies' potential liability.[105] In determining which substantive regulations are necessary, a multi-stakeholder process is crucial to differentiate conduct which may need to be prohibited because it cannot be countered by consumers and conduct necessary for consumers to trust the use of algorithmic decision-making systems.[106] Discussions about proposed regulations should draw on the elements of trust emphasized in the Mayer model—ability, integrity, and benevolence—so as to create robust trust-promoting mechanisms through the use of multiple provisions when one provision may not touch on all three elements.[107]

Additionally, substantive regulations are worthless if not backed with powerful enforcement. Regulators should consider a variety of partners in enforcement, ranging from the federal government to state counterparts to even a private right of action. Such enforcement provisions need not be monolithic; regulators can, for example, allow state agencies to supplement a federal agency's enforcement, but allow the federal agency to consolidate the enforcement action.[108] Similarly, the private right of action may be limited to certain violations to offset concerns that any use of algorithmic decision-making systems could open the floodgates of private litigation.[109]

---

[104] *See* Ripken, *supra* note 35, at 190.

[105] *See, e.g.*, Truth in Lending Act, Pub. L. No. 90-321, 82 Stat. 146 (1968) (requiring disclosures about the terms of consumer credit and standardizing the manner in which costs associated with borrowing are calculated and disclosed).

[106] *See* Ripken, *supra* note 35, at 192.

[107] *See supra* Part II.

[108] *See generally* Elysa M. Dishman, *Enforcement Piggybacking and Multistate Actions*, 2019 BYU L. REV. 421 (2019) (discussing the roles of state attorneys general within the civil "multienforcer" ecosystem in the United States).

[109] *See* Joseph Jerome, *Private Right of Action Shouldn't be a Yes-No Proposition in Federal US Privacy Legislation*, IAPP: PRIVACY PERSPECTIVES (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/ [https://perma.cc/5HPR-JFRF].

While critics of substantive regulation traditionally view this approach as paternalistic and undermining individual autonomy, the past lessons of transparency as the lone mechanism for trust-promotion in the privacy context illustrate that the power differential in modern information relationships already undermines the foundational assumption of equals meeting in the marketplace.[110] Given the failings of transparency as trust in the privacy context and the nuanced role of trust with algorithmic decision-making systems, maintaining and fostering public confidence in the digital economy is paramount, especially where consumers may not have the ability to opt out. By allowing consumers to make informed decisions about algorithmic decision-making systems' trustworthiness and by lowering the amount of trust required to have confidence in these systems, substantive regulation requiring or prohibiting certain conduct should be viewed as *enabling* individual autonomy rather than suppressing individual autonomy.[111]

VI. CONCLUSION

Life is not without risks. However, despite these risks, trust—the willingness to be vulnerable to these risks—enables society to function. Trust-promotion mechanisms can both increase individuals' assessments of others' ability, integrity, and benevolence, and in turn, their trustworthiness, as well as reduce the amount of trust individuals must have before being willing to undertake certain risks. However, as differing approaches in the privacy context demonstrate, such mechanisms must rely on more than transparency alone. Within the privacy context, comprehensive substantive regulation appears to have arrived after consumer trust in the digital economy dropped to an all-time low. Now, as organizations seek to use algorithmic decision-making systems, regulators have the opportunity to learn from the mistakes of the past and govern with substantive regulation in mind at the outset. The use of substantive provisions to augment transparency addresses the limited effectiveness of notice-and-choice, allowing consumers to cast aside eroded trust in the digital economy. This approach would instead allow consumers to move beyond simply dealing with the devil they know; it would renew confidence in the digital economy as we move into the algorithmic age.

---

[110] *See supra* Part III.B.2.A.

[111] *See* Ripken, *supra* note 35, at 200 (2006) ("The law, therefore, should not be seen as an intrusive device that inhibits market activity, but an organizing mechanism that promotes robust market participation. The coercive force of substantive law creates orderly markets which then facilitate individual transactions.").