The Notice-and-Choice Privacy Gamble: Game Theory, Consumer Agency, and Implications for GDPR

Matt Hettche
Christopher Newport University

Dae-Hee Kim
Christopher Newport University

Michael J. Clayton
American University

This article provides a theoretical basis for why the notice-and-choice model for protecting consumer information privacy might still be considered a viable policy approach despite evidence that privacy notices are often ignored, difficult to read, and misunderstood by consumers. Drawing from several well-known game-theoretic models that map closely to an online consumer's notice-and-choice context, we outline a rational choice model for consumer online privacy and discuss its relevance for the EU's General Data Protection Regulations [GDPR]. We argue that an online consumer's notice-and-choice privacy gamble is a reasonable bet when constrained by competition and the presence of meaningful regulation.

Keywords: consumer agency, game theory, general data protection regulation, notice-and-choice privacy notices

INTRODUCTION

Placing a reasonable bet under conditions of uncertainty is not a completely foreign experience for most consumers. Trial and error, probabilistic inference, and needing to make a best guess with the available information are typical of many consumer situations (Urbany et al., 1989). While there is no shortage of examples of where consumers are constrained by asymmetric information, bounded rationality, overconfidence, or any number of systematic or cognitive biases, there are, perhaps reassuringly, other well-worn examples of consumer autonomy within efficient markets that have come to typify the digital economy (Fracassi & Magnuson, 2021).

Privacy notices and the requisite checkbox action to "acknowledge-and-continue," although ubiquitous to the consumer's online experience, are proving to be increasingly difficult for privacy and marketing scholars to justify as a matter of sound business policy (Warner, 2020). While there is little disagreement that information disclosure and consumer choice remain basic components of informed consent, there is a growing body of evidence that suggests privacy notices simply fail to provide consumers with sufficient information for an actual informed privacy choice (Ke & Sudhir, 2022). Privacy notices are often ignored,

considered difficult to read, increasing in length, difficult to comprehend, or fundamentally misunderstood (Calo, 2012; Milne & Culnan, 2004; Nissenbaum, 2011; Warner, 2020). What, if anything, do privacy notices provide for a consumer's choice in the context of a notice-and-choice transaction? Is the checkbox action to acknowledge-and-continue a completely meaningless or empty gesture, given that consumers do not read, hardly read, or fundamentally misunderstand the conditions to which they volunteer personal information (Martin, 2015)? Or worse, are consumers systematically deceived, coerced, or perhaps simply conditioned to surrender personal information without recognizing the short and long-term implications of their actions (Walker, 2016)?

This article aims to outline a theoretical basis for why the notice-and-choice model can stand as a viable consumer protection mechanism for online privacy by addressing persistent worries about notice adequacy and information disclosure. Drawing from game theory and a theory of consumer agency that we believe to be implicit in the EU's General Data Protection Regulations [GDPR hereafter], we aim to explain how consumer choice, as a deliberate action, is the result of a rational and experiential process that is constrained by competition and dynamic forces of institutional trust. Game theory provides a useful forum for evaluating privacy-related decision-making because it introduces a set of concepts and distinctions that frame a consumer's expectation for privacy protection in terms of subjective degrees of belief and a theory of revealed preference.

In broad outline, we argue that the mere presence or instantiation of a consistent and complete privacy notice, independent of whether it is actually read and fully understood by a given consumer, affords conditions whereby the consumer can subjectively evaluate conditions for institutional trust alongside the perceived benefits of future information transactions and their potential privacy-limiting implications. This is what we refer to as the consumer's "privacy gamble." We argue further that consumer choice, in the context of an online notice-and-choice transaction, is a signifying action that brings about or creates reciprocal duties and responsibilities for consumers and data controllers alike.[1] Provisions within GDPR, such as requiring better privacy notice communication protocol and providing consumers the opportunity for data access and deletion, are consistent in their intent with our interpretation of consumer agency and consumer choice. In our discussion, we conclude with suggestions for future research on how the notice-and-choice model can be further integrated into the implementation of GDPR by considering additional choice-theoretic derivations or games from a consumer and firm institutional trust perspective.

The current discussion contributes to the field of marketing and public policy research by offering a theoretical framework and basis for the notice-and-choice model as a current consumer protection policy approach emanating from the EU. Although there are some prior studies that examine how game theory can be used to clarify privacy research, this is the first effort that we are aware of to explore the theoretical underpinnings of GDPR and its embrace of notice-and-choice as a consumer protection policy.

CHALLENGES TO THE NOTICE-AND-CHOICE MODEL

The notice-and-choice model draws its primary fire from critics on the issue of information disclosure. The worry, in a nutshell, is that if consumers do not understand or appreciate the details of a privacy notice, there is no legitimate sense in which they can choose, agree, or consent to the conditions of an information exchange (Slepchuk & Milne, 2020). Since a consumer's knowledge is partial or incomplete, any privacy-related decision is null and void. Nissenbaum (2011) criticizes the model as follows: "notice-and-consent . . . [contains]. . . a fundamental flaw, namely, its assumption that individuals can understand all the facts relevant to true choice at the moment of a pair-wise contracting between individuals and data gathers" (Nissenbaum, 2011, p. 32). Skeptical of attempts to refine or improve notice-and-choice, which by implication includes the EU's GDPR, Nissenbaum (2011) offers an alternative set of decision heuristics derived from a "theory of contextual integrity" (Nissenbaum, 2011). The appeal to context, although not completely unproblematic, is certainly intriguing and has consistently made its way into recent marketing and public policy discussions on privacy (Acquisti & Grossklags, 2005; Martin, 2015; Walker, 2016). Context aims to isolate the relative interests and circumstances of interested parties so that privacy-related decisions can be clarified and made determinate. Context, therefore, modifies both the instrumental or ends-

related choices a consumer makes about her situation or well-being and the epistemic conditions surrounding the information or notice she needs for informed consent.

Often contrasted with the "harm-based model," where privacy notices serve as de facto disclosure documents to inform consumers of potential physical or economic harm that may result from the information exchange process, the notice-and-choice model highlights consumer autonomy and transparency (Muris, 2001). With notice-and-choice, information about data collection, use, access, confidentiality, and third-party sharing (the classic FIPPS in the US Federal Trade Commission's guidelines) are publicly available to anyone interested in transacting with a given data controller or processor (Peltier et al., 2010). Privacy notices serve as the *raison d'être* for privacy and consumer watchdog groups to audit and monitor exploitive practices (Peslak, 2005; Thierer, 2013; Slepchuk & Milne, 2020). Insofar as data controllers and processors are compelled to provide and act in accordance with detailed up-front policies, internal standards, at least in theory, can be evaluated post hoc for consistency, effectiveness, and fairness. Ohlhausen (2014) suggests that the harm-based model and notice-and-choice, when taken together, complement one another and, while not perfect, stand as an effective consumer projection policy approach (Ohlhausen, 2014). Threat of significant punishment and clear standards for compliance, as we shall see, are cornerstones of GDPR and conform likewise to the broader commitments of consent and transparency present in a dovetailed policy approach (Ruohonen & Hjerppe, 2022).

The question of whether notice-and-choice can or should stand independently from the harm-based model is not an issue we explore or consider in-depth in this article. Following Ohlhausen 2014, we simply assume that the two models stand together. Similar to notice-and-content, the harm-based model requires notice adequacy and information transparency, but it also involves additional considerations about a firm's compliance and issues related to enforcement, such as composite decision-making and administrative protocol (Gentile & Lynskey, 2022). Insofar as we tacitly assume the harm-based model as operative and "in play," we willingly admit our proposed theoretical framework for the notice-and-choice model is narrowly focused and aims primarily to address concerns about consumer knowledge and access to information.

INFORMATION DISCLOSURE AND THE AGENCY MODEL OF CONSUMER-CHOICE

The question of the extent and scope of consumer knowledge as it relates to notice-and-choice is neither trivial nor simply restricted to the privacy realm. Manson and O'Neill (2007) for example, discuss the issue of information disclosure in the context of medical informed consent and offer two contrasting notions of information transfer that are useful for our discussion. First is information transfer as a "container/conduit" model, and second is information transfer as an "agency/communicative" model (Manson & O'Neill, 2007, p. 26). Under the container model, information is regarded as discrete packets or objects that can be transferred from one container or person to another. In this view, information is supplied and received in a mechanical and piecemeal fashion so that once the consumer/patient, as a passive receptacle, receives sufficient information, she can properly agree or consent to the terms and conditions of a given transaction.

The agency/communicative model, in contrast, regards the act of informing as "referentially opaque" insofar as what is said, or what is spoken, and what is heard may or may not be the same (Maclean, 2009, p. 136). What the informer intends and what the informant interprets depend on a set of contingent conditions, such as conscious beliefs, background knowledge, and prior experience. Essential to the agency model of consent, therefore, is mutual engagement in a communicative process (Manson & O'Neill, 2007). Maclean (2009) explains that under the agency model, "consent is not simply the state of mind of the person giving consent but engages two persons, both of them agents with rights, responsibilities, and duties" (Maclean, 2009, p. 137). What the consumer/patient knows, understands, and decides about a transaction, therefore, is part but not the only part of a larger and extended process.

The notice-and-choice model, when narrowly interpreted through a container/conduit metaphor, in contrast, over-emphasizes the role of information transfer and its content for a consumer-choice decision. While it is certainly true that the consumer must know something about the terms and conditions of a data exchange, neither a complete nor comprehensive understanding of a firm's privacy notice is required. To

use an analogy from the medical field, in order to consent to a medical procedure, a patient need not possess a detailed understanding of the procedure's mechanics or process, have the complete work histories and safety records of those involved, and weigh the scientific evidence that supports the procedure's likelihood for success. These things are indeed important, in principle knowable by the patient, and are presumably reviewed by experts and patient advocates alike; however, as discrete packets of complete information that are transferable to the mind of the decision-making patient, they are simply not required for an informed choice. That a patient is able to acquire a generalized understanding of these things is, in truth, ancillary to the related decision about whether to trust the doctor, hospital, and medical professionals who perform the procedure.

Returning to the notice-and-choice model (as a consumer privacy protection approach), it is therefore vital that full disclosure of a firm's privacy policy is made publicly available and that it is reviewed, or at least reviewable, by privacy experts and consumer advocates. The important takeaway here is that somebody, at least in principle, reads the firm's privacy notice, and the notice itself is presented as a coherent, consistent and complete statement of a firm's data handling protocol. However, whether a given consumer personally consults a particular privacy notice in full, understands the scope and extent of the data collecting and sharing protocol, or appreciates the short and long-term risks of sharing personal data is (again) ancillary to the related decision of whether to trust the data controller. As a consequence, the notice-and-choice privacy gamble is fundamentally a choice about institutional trust and cannot simply be reduced to a consumer's knowledge of a data controller/processor's data collection, use, and sharing protocol. Acquiring a generalized understanding of a controller's data policy may, of course, be the result of directly studying a firm's privacy statement. Moreover, a cogent presentation of a firm's data policy may, in fact, prompt or engender consumer trust (Tang et al., 2008; Ermakova et al., 2016). However, it is not at all likely that a consumer-choice decision will result solely from an isolated information-transfer event prompted by the presentation of a firm's privacy notice. At the very least, there are background beliefs and contextual clues that shape and inform a consumer's choice in addition to any generalized or specific knowledge gained from reading a firm's privacy notice.

Yet before outlining the theoretical framework that warrants notice-and-choice as a rational and therefore viable consumer policy, let us first briefly review the structure and key elements of GDPR and consider how it relates to consumer agency more broadly.

THE EU'S GENERAL DATA PROTECTION REGULATION

In contrast to the US's patchwork system of regulations to safeguard consumers' information privacy, which is sector- and region-based, the EU operates as a supranational legal system, wherein all member states adhere to a common set of regulations with the aim of providing consistent standards for a single market (Menon, 2019). GDPR is a comprehensive policy that specifies the rights of "data subjects" as well as the corresponding obligations of "data controllers" and "data processors" (Tamburri, 2020). It applies to all EU citizens and any company, website or organization transacting with EU citizens (Schweigert & Geyer-Schulz, 2019). GDPR was adopted in 2016, enacted into law in 2018, and formally replaced the 1995 Data Protection Directive, Directive 95/46/EC (Menon, 2019). GDPR is sometimes referred to as an "innovation shaping law" insofar as it is global in scope, emphasizes the rights of individuals, and requires organizations to engineer data security into the very conduct of their business practice (i.e., embrace what GDPR calls "privacy by design and default") (Godinho de Matos & Adjerid, 2022; Tamburri, 2020).

The structure of GDPR, as a policy document, is comprised of 99 articles, spanning 261 pages, and is roughly divided into four unequal parts: (1) assumptions, terms, definitions and principles (Articles 1 - 11); (2) rights of the data subject (Articles 12 - 23); (3) obligations of data controllers and processors (Articles 24 - 43); and (4) the policy's contingencies and administration (Articles 44 - 91) (European Parliament and of the Council, 2016). Fundamental to GDPR's material scope is the idea that a natural person (i.e., any living person) possesses and creates data in the execution of their own life and is therefore afforded a claim right to their personal data. Data subjects, who are EU citizens, have legal protections that govern the permission, access, and focus of data collected, used, and processed on their behalf (Schweigert & Geyer-

Schulz, 2019). For the purposes of GDPR, defining "data subject" in terms of a "natural person" is indeed significant. By fiat, corporations, organizations, and governmental agencies, mere legal persons, do not meet the criteria for legal protection. Deceased individuals, similarly, insofar as they are not living, are not afforded the same protections and powers under the regulation.

Moreover, the type of information deemed personal by GDPR is not simply limited to individuating identifiers, such as a name or identification number. Psychographic information, including values, religious or philosophical beliefs, cultural and social identities as well as behavioral information, including geographical location, economic histories, and purchase status are also explicitly protected (Article 4). According to GDPR, data subjects are beings in the world, real people, with interests, goals, and lives to live (Breen et al., 2020). The rights outlined in Articles 12 – 23, therefore, aim to empower individuals clarifying conditions for consent as well as the specific powers subjects possess to gain access to their personal data, to correct any errors connected to their data, and move, transfer, or delete data that are warehoused on their behalf (European Parliament and of the Council, 2016). These stipulations outline the legal expectation of reciprocity that exists between data subjects and data controllers/data processors (Breen et al., 2020). At its core, GDPR aims to establish the boundaries, limits, and expectations for those wishing to transact and maintain relationships with data subjects (Ke & Sudhir, 2022). In the context of notice-and-choice privacy notices, information transfer and consent are not simply assumed from a checkbox action and clicking "submit" or "agree." Per GDPR policy, notices must be written in "concise," "clear," "accessible," and "plain" language (Article 12). Consent is considered both ongoing and revisable, but it is also not considered indefinite. In the parlance of the policy, data subjects have the "right to be forgotten" (Article 17).

The legal obligations of data controllers and data processors are also a central component of GDPR. A data controller is defined as an entity or organization that "determines the purposes and means of processing personal data." (Article 4, para 7). Contrasting, for example, earlier US attempts to outline consumer information privacy protections, such as the 2012 Obama Administration's Consumer Bill of Rights, where specific reference is made to "data companies" and business, GDPR's target is much more general and inclusive, recognizing natural persons, legal persons, organizations and agencies alike (Anonymous, 2013; Article 4). Within GDPR, data processors are defined as surrogates of the data controller who, quite simply, "process personal data on behalf of the controller" (Article 4, para 8).

GDPR articulates explicit requirements for controllers to not only "be accountable and demonstrate compliance" (Article 24), but also proactive to inform data subjects about real and suspected data breaches (Article 34), prepare regular privacy impact assessment reports (Articles 35 & 36), and when large-scale processing and data monitoring are involved, controllers must appoint a Data Protection Officer or ombudsperson to ensure full-fledged compliance with GDPR policy (Articles 37, 38, 39). These provisions ultimately aim to reinforce mutual engagement between data subjects and controllers in a communicative process that underscores consumer agency and consumer choice. More so than prior policy attempts, GDPR outlines an array of inbound services that data controllers need to provide, and which need to remain time-sensitive and transparent (Menon, 2019).

Above all else, GDPR garners salience for business organizations and public agencies by virtue of its guidelines for administrative fines and penalties (Ruohonen & Hjerppe, 2022). In addition to candid descriptions about potential civil liabilities for material and non-material damages (Article 82), GDPR provides precise recommendations for data processors who fail to act and comply with written policy. The often cited 20-4 rule stipulates, for example, that data controllers face stiff fines of either €20M or 4% of global turnover (whichever is larger) when not adhering to the rights outlined on behalf of data subjects (Article 83). Additionally, data controllers are also required to monitor the conduct of other third-party data processors when outsourcing data services (Article 28). Failure to comply with these and other administrative processes of GDPR have similar stiff penalties for data controllers, resulting in €10M or 2% of global turnover, again whichever is larger (Article 83).

Enforcement of stiff penalties, and the aftermath of several high-profile prosecutions, arguably prompt social conditions that favor industry-level compliance (Zaeem & Barber, 2020). Moreover, recent empirical evidence suggests that GDPR not only has positively impacted the quality of privacy policy notices for

consumers internationally (Zaeem & Barber, 2020) but also that globally data controllers (websites) have substantially reduced interactions and data sharing with third-party vendors (Peukert et al., 2022; Gal & Aviv, 2020). The size and quality of the EU's consumer markets have elevated expectations for data subject rights, prompting similar regulative approaches in various US territories. Five US states, including California, Virginia, Connecticut, Colorado, and Utah, have enacted comprehensive data privacy laws with provisions for data subjects to gain access and control over their data and more states are anticipated to do so in the near future (Bloomberg Law, 2023).

In the next section, we aim to provide an account of consumer agency and choice from a rational economic perspective. We aim, in particular, to describe the context from which consumers can rationally consent and agree to informed informational transactions. Using game theory and expected utility theory, we delineate the formal conditions that surround a consumer's privacy gamble and highlight various strategies that lead to different game theoretical outcomes or solutions. After reviewing some of the basic elements and assumptions of game theory, we will turn to consider four simple games that map well to a consumer's notice-and-choice privacy context.

GAME THEORY AND THE PRIVACY GAMBLE

Prior attempts to use game theory to inform consumer privacy-related decision-making are isolated to mainly two studies: (1) Acquisti and Grossklags (2005), where general and specific consumer privacy concerns are framed in the context of incomplete and asymmetric information; and (2) Vila et al., (2003), where privacy concerns in as e-commerce context is described as lemons market with signaling (Barth & de Jong, 2017; Kokolakis, 2015). To the best of our knowledge, the following analysis is the first attempt to analyze the situational context of notice-and-choice transactions using game-theoretic models. And while the games we review are relatively simple (finite extensive-form games of perfect information), their descriptions and solutions are aptly mapped onto the situation in which consumers find themselves.

According to Ross (2016), there are essentially three conditions that certify a player as an "economically rational agent:" (i) the player can assess various outcomes of the game through a rank ordering of preferences (i.e., the player possesses a "utility function" of revealed preferences; (ii) the player can identify various strategies of play that depend on the decisions and choices of others (i.e., the player can consult and have access to the game's "payoff table"); and (iii) the player can choose among the possible strategies of the game and choose one as the best or equal to the best that maximizes his/her expected utility (i.e., the player can arrive at a "solution" or "equilibrium" of the game) (Ross, 2016, p. 8). The four games described below are finite, non-zero-sum, sequential-move games with two players, each with perfect information. Each game is finite in that each game will end or terminate after a known number of actions or moves (in our case, M = 2), and each game is non-zero-sum in that the winning strategy of player one does not depend on the non-winning strategy of player two and versa vice (such as a of the game of tic-tac-toe), and the strategies, payoff, and choices of each player are not hidden from the other. The provision of perfect information is essentially a constraint on the game's logical structure and entails that the preferences, payoff, and moves during the game are known and transparent to each player.

Four Simple Games

The first game is called the Privacy Gable, and it roughly models the type of consumer choice problems experienced in an online digital marketing context. In this case, player one, Alice, the consumer, finds herself confronted with a notice-and-choice transaction prompted by the privacy notice of player two, Bob (the company/data controller). The decision dilemma is admittedly simple and assumes Alice neither reads nor attempts to understand Bob's lengthy privacy notice but must decide if she wants to "acknowledge" the terms of the policy nonetheless and continue with a more robust information exchange. Alice has the game's first move and must decide whether to trust Bob with her information (i.e., opt-out). However, she also knows Bob's choice, a potential second move of the game, is contingent on her trusting him, a move that also potentially leads to her own exploitation. Assume, for the sake of argument, that Alice knows or can

appreciate what it means to have her privacy violated and information exploited by Bob. The ordinal utility functions for each player are as follows:

TABLE 1
ORDINAL UTILITY FUNCTIONS FOR PRIVACY GAMBLE

Player A (Alice):	Trust >> 2; Opt-Out >> 1; Exploited >> 0
Player B (Bob):	Exploit >> 2; Respect >> 1; Opt-Out >> 0

Bob's action to exploit need not imply an immediate direct harm to Alice. However, it does entail unrestricted access to use and derive benefit from Alice's information as Bob sees fit. And while it is true Bob has provided a nominal assurance to respect Alice's privacy via the privacy notice and consent agreement, Bob's maximum utility (i.e., best-case outcome) is only realized after Alice chooses to trust and Bob, likewise, to exploit.

TABLE 2
PAYOFF COMPARISONS FOR PRIVACY GAMBLE

		Bob	
		respect	exploit
Alice	opt-out	1 , 0	1 , 0
	trust	2 , 1	0 , 2

The number left of the comma refers to A's (B's) preference ordering
(0 = worst outcome; 2 = best outcome)

Before discussing the solution to our first game (Privacy Gamble) and what is considered rationally consistent for each player to choose, given each player's revealed preference and anticipated payoff, it will be helpful to review another virtually identical game-theoretical model called Kidnap attributed to Daniel Ellsberg (the Harvard trained statistician and RAND Corporation game-theorist who later, as it turns out, leaked the Pentagon Papers to the New York Time in 1971) (Binmore, 2007). Like our prior game, Ellsberg's Kidnap is a finite, non-zero-sum, sequential-move game with two players and perfect information. The comparison payoff table is nearly identical to the Privacy Gamble; the only differences are the player's action descriptions as well as minor details with the initial context.

TABLE 3
PAYOFF COMPARISONS FOR ELLSBERG'S KIDNAP

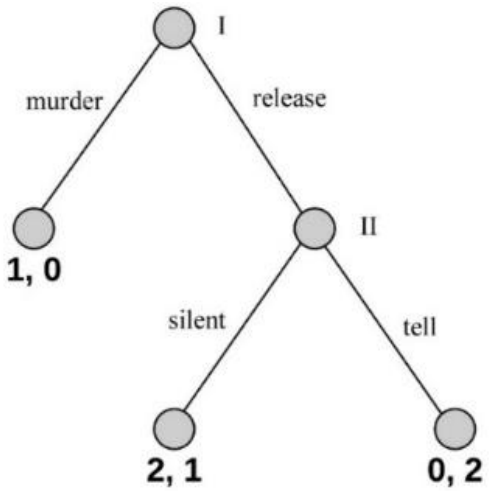
		Bob	
		silent	tell
Alice	murder	1 , 0	1 , 0
	release	2 , 1	0 , 2

The number left of the comma refers to A's (B's) preference ordering
(0 = worst outcome; 2 = best outcome)

Here, Alice is not nearly as innocent as in the prior game and has kidnapped Bob. Yet luckily for Bob, a ransom has been paid, and Alice must now decide if she will set him free or murder him. Alice clearly prefers not to be a murderer and have to dispose of Bob's body, but she also sees a clear risk in letting Bob go since he could easily reveal her identity to the police and jeopardize her future. Very similar to Bob's nominal promise in the Privacy Gamble, Alice must decide if she can trust Bob and his reassurance to stay quiet (in the event of his release) when making her first and only decision of the game.

An alternative method for representing sequential-move games, also called "extensive-form games," is the directed graph or game tree.

FIGURE 1
GAME TREE FOR ELLSBERG'S KIDNAP



Moving top to bottom, each player's decision node is labeled I or II and each potential terminal node of the game lists each player's expected payoff accordingly. The first number refers to player one's expected payoff and the second number to player two's expected payoff. Represented as a directed graph, Ellsberg's Kidnap reveals information about the game's structure and players' sequences of play that are obscured when simply consulting the game's payoff table (Table 3, above). Moreover, an effective technique applied to a directed graph to demonstrate the game's solution, using backward-induction analysis, is a method called "Zermelo's algorithm" (Ross, 2016; Schwalbe & Walker, 2001). It works as follows: working backward, from bottom to top, we isolate player two's (II) final potential decision as a choice between (tell >> 2) and (silent >> 1). Since Bob's strategy "tell" is at least as good as his alternative, "silent," we can resolve this subgame by canceling or deleting the game's (2, 1) payoff strategy, thereby leaving player one's (I) choice between (murder >>1) and (tell >> 0) (Binmore, 2007). Since Bob's only option is "tell" in the reduced game and Alice prefers "murder" to "tell," the game's solution (i.e., its Nash equilibrium) is "murder," "tell." This solution, "murder," "tell," not only turns out to be the solution to the entire game, but it is also the solution to all of the game's subgames as well. In fact, both Ellsberg's Kidnap and the Privacy Gamble retain what are called "subgame-perfect equilibria" (SPE) solutions. For our prior game, the Privacy Gamble, the solution is "opt-out," "exploit," and we can conclude that given the revealed preferences (currently) assigned to Alice and Bob, as well as our prior analysis of their payoff strategies, it would be inconsistent for either player to choose anything other than "opt-out," "exploit."

Yet to see how the Privacy Gamble may have a different solution outcome and how there is a game theoretic model that is most typically applicable to an online consumer's notice-and-choice context, let us now consider a third game presented by Binmore (2007) called Cosy Kidnap. The initial conditions of Cosy Kidnap track closely with Ellsberg's Kidnap: Alice has kidnaped Bob and, in the first move of the game, must decide whether to murder or release him. In fact, Alice's revealed preferences in this game are exactly as they were before. She strongly desires that Bob not tell and prefers not murdering to murdering Bob. Alice's utility function is as follows: (release >> 2; murder >> 1; tell >> 0). Bob's preferences in this new game, however, are different. Struck with an incidence of "Stockholm syndrome," Bob now develops real and positive feelings for Alice and reverses his previously revealed preference for telling and remaining silent.

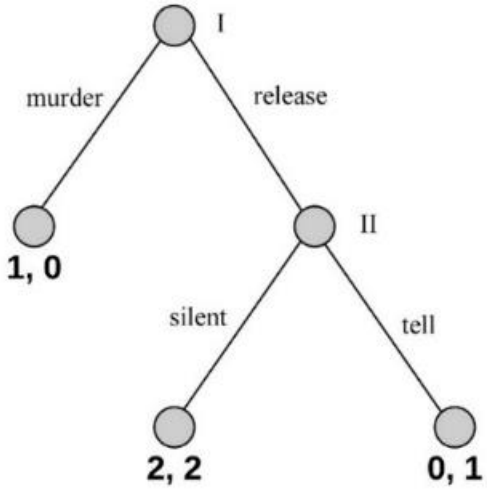
TABLE 4
PAYOFF COMPARISONS FOR COSY KIDNAP (BINMORE, 2007)

		Bob	
		silent	tell
Alice	murder	1 , 0	1 , 0
	release	*2 , 2	0 , 1

The number left of the comma refers to A's (B's) preference ordering
(0 = worst outcome; 2 = best outcome)
*indicates the game's equilibrium solution

Bob's newfound affection for Alice is significant because it represents a refinement of our initial game of Kidnap. Insofar as Bob's preferences are transparent to Alice, he clearly prefers remaining silent to telling and thereby forces a different "subgame perfect equilibrium" (SPE) solution (Binmore, 2007). Provided that both Alice and Bob are rational players with perfect information, it is a safe bet that Bob will play silent as opposed to telling if Alice were to choose release. And since Alice is rational as well as self-interested, she will choose release over murder since the former has a higher payoff than the latter, and she trusts that Bob will not select the rationally inferior choice in the game's closing move.

FIGURE 2
GAME TREE FOR COSY KIDNAP



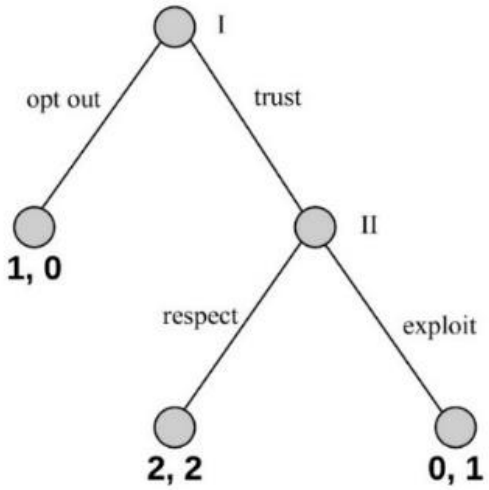
The refinement made to the game of Kidnap anticipates another refinement we can make to the Privacy Gamble game, similarly along the lines of adjusting player two's (Bob's) preferences. In this revised version of the game, what we call the Privacy Gamble Redux, Alice's revealed preferences are the same as before, but Bob reverses his ordered preferences from exploit to respect in the following fashion: (respect >> 2; exploit >> 1; opt-out>> 0). Struck this time not with an incidence of Stockholm syndrome but with what we might call "Apple-Really-Cares syndrome" (tongue-in-cheek), where Bob's concern and care for user/member data are outwardly expressed, and the motive to exploit consumer data is sharply attenuated. The comparative payoff table and extensive-form game tree are, therefore, as follows:

TABLE 5
PAYOFF COMPARISONS FOR PRIVACY GAMBLE REDUX

		Bob	
		respect	exploit
Alice	opt-out	1 , 0	1 , 0
	trust	*2 , 2	0 , 1

The number left of the comma refers to A's (B's) preference ordering
(0 = worst outcome; 2 = best outcome)
*indicates the game's equilibrium solution

FIGURE 3
GAME TREE FOR PRIVACY GAMBLE REDUX



Recall that in the Privacy Gamble, Alice (the consumer) must decide in the opening move of the game whether to trust Bob (the data controller) with an "acknowledge-and-continue" action that typifies a notice-and-choice transaction. Similar to the game Cosy Kidnap, the Privacy Gamble Redux has a "subgame perfect equilibrium" (SPE); in this case "trust," "respect." The implications of this refinement to the Privacy Gamble (i.e., revising Bob's preferences) is that the consumer's gamble to accept the terms and conditions of a firm's privacy policy is rationally consistent, even if the consumer foregoes reading the privacy notice itself. In the parlance of game theory, the privacy notice is simply "cheap talk," a mere signal, and what really matters is knowledge, or more precisely, perfect information about each player's expected payoff. Granted, the case for how and why Bob is plausibly struck with an instance of Apple-Really-Cares syndrome, sufficient to garner Alice's trust, is certainly not a trivial assumption and will require a fuller or extended discussion below. Yet before turning to that discussion, we will first review two other, perhaps more fundamental, objections that befit our account.

Objections and Replies

The first objection, not uncommon anytime game theory is applied to the problems and issues of social science, is that the games presented (above) assume that the players are "purely" or "economically" rational, which in the real world they are not, so any conclusion or argument offered from a game-theoretic perspective is untenable. The world is a messy and unpredictable place, the objection goes, and what makes sense in theory simply does not apply to the real world. This objection questions how conclusions arrived

at in a hypothetical or idealized context must, by necessity, relate or apply to everyday concrete human experience.

To reply, it is well worth pointing out that game theory is a purely formal (mathematical) discipline with no substantive content of its own (Binmore, 1994). Players' preferences and their strategies are analyzed for consistency from various assumptions that may or may not find an analog in the real world; that is true. Yet to say game theory has no application to the real world is tantamount to saying that humans, and the many games that befit social life, are never rational. And this is certainly too strong. While it is certainly true that humans are often, even predictably, irrational, this is not to say that humans are and can be rational actors. Recall the central conclusion we offer in this present article is that consumers are not acting irrationally or inconsistently when they do not read or do not fully understand the privacy notices to which they consent and agree. To deny the economic rationality of online consumers simply begs the question of our central argument.

A second objection that can be offered against our analysis of the Privacy Gamble draws into question the set of game-theoretic models selected for illustration and discussion above. The objection, put succinctly, is that the games presented are much too simple and do not map onto the complicated world of a consumer's privacy-related decision-making context. The games are one-shot, two-player, sequential-move games with perfect information, much too simplistic to reflect the range of complex social relationships that constitute an online consumer's information-sharing reality. Walker 2016, for example, points out that "exchanges of information on the Internet rarely occur in a simple, dyadic relationship between one party and another. Conversation and interaction online are often a complex (web) of information and algorithms" (Walker, 2016, p. 150.) Acquisti and Grossklags (2005) note further in "information asymmetries. . ., for example, how personal information will be used—might be known only to a subset of the parties making a decision" (Acquisti & Grossklags, 2005, p. 26). Calling into question both the logical structure of the Privacy Gamble (as a game) as well as assumptions about the player's access to information undoubtedly puts pressure on our account.

In response to this second objection, it is important to clarify a general point about the notion of informational privacy and how it relates to the context of a consumer's privacy expectations or preferences. Informational privacy, as a notion or concept in the abstract, is indeterminate and vague. This is not to say there are not clear instances where a person's information is vulnerable to exploitation; however, it does mean, without sufficient context to define the relative interests and goals of interested parties involved, and exactly how and why a piece of information creates a vulnerability, there will be borderline cases for what is deemed privacy-worthy and privacy-unworthy. Note this indeterminacy is not simply a matter of not knowing certain facts or having access to certain information. The situational context for realizing a consumer's preference is simply left open and undecided.

It is precisely because of the vague nature of informational privacy that the appeal to institutional trust becomes so important and definitional to a consumer's privacy gamble. Whereas more information about a data controller's data handling protocol may impact a consumer's assessment of institutional trust, it may also have no impact at all. The point here is that no amount of information (save clairvoyance) will stabilize a consumer's privacy preference or expectation from one context to the next. What is elemental, however, is a decision, made in uncertain conditions, about the intentions and revealed preferences for mutual engagement in a trusting relationship. The privacy gamble is therefore predicated on institutional trust (not simply informational disclosure), and the simple game structure posed above captures this intuition.

INSTITUTIONAL TRUST AND IMPLICATIONS FOR GDPR

The solution to the Privacy Gamble Redux depends in a crucial way on defending the refinement of what we have called Apple-Really-Cares syndrome, where the firm or data controller's revealed preference is to respect rather than exploit a consumer's transacted data. Reasons to believe that this is a reasonable or plausible refinement to the proposed game (above) arguably rely on three considerations. First, compliance and enforcement mechanisms, such as those implicit in the harms-based model, as well as what is assumed in GDPR regulations, prompt exogenous or external pressure for data controllers to act in accordance with

respecting a consumer's data. While not sufficient in and of itself, a competent regulative system will deter exploitive action from a firm/data controller by placing financial risk and administrative penalties in play. In recent years, several Big Tech companies, such as Apple, Meta/Facebook, and Google, have publicly conceded that some form of regulation is needed, given the scope and unpredictability of misappropriating consumer data. The State of California, with its Consumer Digital Privacy legislation, and as mentioned above, at least four other US States have adopted GDPR-inspired privacy regulations that empower data subjects and impact the use of notice-and-choice, such as requiring more concise and user-friendly privacy policy statements as well as providing options for consumers to access and potentially delete data related to their online transactions. Whereas these new laws and regulations raise questions about effective and realistic enforcement, early indications of industry compliance signal an increased concern and sensitivity for respecting a consumer's data.

A second reason for endorsing an Apple-Really-Cares syndrome type-refinement has to do with the role of competition among data controllers and processors. This dynamic force in the market has the potential to cut in two different directions, however. On the one hand, competition can, in theory, spawn good behavior among firms and data gathers, where firms can take a stewardship role in defining privacy principles or articulating how respecting consumer privacy is consistent with core values or missions. As consumers learn to value their own informational privacy and, perhaps, begin to see the potential long-term harm resulting from carelessly attending to their own data privacy needs, those companies and firms with comprehensive and coherent data handling strategies will benefit from increased customer loyalty and patronage. Yet, on the other hand, it should be noted competition can also spawn bad behavior for misappropriating and exploiting consumer data. This can be described as a type of snowball effect. Once a company and then another find ways to compromise consumer data privacy, industry standards reduce to the lowest common denominator. Within the context of privacy notices, for example, the complexity and even length of one company policy may prompt and encourage more complexity and more length from another.

In the absence of regulation or meaningful regulation, competition is certainly susceptible to encourage exploitive data practices. However, insofar as competitive forces are also impacted by an industry's attempt at compliance, the two can work in tandem to support institutional trust. Briefly put, institutional trust is prompted by several forces operating in the market and relies on not only consumer protection and enforcement but consumer education as well. One vital area of marketing and privacy research to develop is identifying ways to broaden consumer understanding and knowledge about information sharing and privacy protections (Walker, 2016). This is not to say, however, that consumer education can replace a coherent and complete privacy notice supplied by a firm/data controller. But having the opportunity to develop personal privacy principles and standards is the sort of thing that manifests as a duty or responsibility when consenting in accordance with a theory of consumer agency. The most obvious provision of the EU's GDPR provisions where consumer education will come to bear is related to data access and deletion requests. Some care and caution will be required that consumers understand and truly benefit from exercising these (not necessarily new) legal rights. One common observation and sometimes complaint from consumers about the roll-out of the new GDPR privacy policies is that while they profess to be more concise, easier to read, and utilize plain language, those notices themselves appear to be more like pop-ups and intrusive ad devices. That is to say, in an effort to appear more respectful and compliant to consumer privacy, firms and data controllers are actually intruding, nay invading, a certain level of consumer privacy. Whether or not this is a temporary element of GDPR's implementation remains to be seen.

The third and final reason firms/data controllers are prompted to accept something like an Apple-Really-Cares syndrome type-condition is one of the very elements that place game theory as a plausible theoretical device for studying and understanding consumer privacy in the first place, namely uncertainty (itself). The idea here is that Privacy Gamble, although illustrated as a one-shot game, is certainly predictable and could be iterated on a number of occasions to include another aspect of a firm's decision dynamic. The uncertainty, for example, of not proactively attending to consumer data, so say confronting the malfeasance of rouge third-party actors, places firms/data controllers in a position of vulnerability. Note

that the uncertainty that we find important is not the imperfect knowledge about a consumer's privacy gamble but rather the uncertainty of not abiding by regulatory or competitive norms for handling and respecting consumer data. In this respect, following something like the weak analogy of Ellsberg's Paradox, firms/data controllers as relational agents will exhibit a form of "ambiguity aversion" where they will prefer the known odds of compliance (the devil that they know) and respect/not exploiting consumer privacy to the alternative (the devil they don't) since supporting a system of institutional trust has more predictable outcomes (Kovářík, 2016). Piecemeal regulation for technologies and industries that have a global reach presents challenges for regulators and businesses alike. Compliance strategies, therefore, can range from partial adoption, adoption, wholesale avoidance, and even transformation (Voss & Houser, 2019). In short, the dynamism of the competitive environment, one predicated on risk avoidance and anticipating some evolution of guardrails or system of consumer protections in the foreseeable future, is sufficient to support an Apple-Really-Cares syndrome type-refinement, therefore, lending credence to our game theoretic analysis.

CONCLUSION

The focus of this present article has been to defend a version of the notice-and-choice model from persistent worries raised in the literature about notice adequacy and information disclosure. Drawing on game theory and a notion of consumer agency implicit in the EU's GDPR, we have attempted to explain how consumer choice is a deliberate action resulting from a rational and experiential learning process related to institution trust. A consumer's privacy gamble involves subjectively evaluating conditions of institutional trust alongside the perceived benefits of future information transactions and their potential privacy-limiting implications. This gamble, while requiring a generalized understanding and knowledge of a data controller's data handling policy, also relies on maintaining a communicative and ongoing relationship with the data controller. Isolating or restricting the context of evaluating privacy in a game theory context remains an important conclusion for understanding the notion of consumer agency.

There are several avenues possible for future research on rational choice theory and privacy. Expanding choice-theoretic derivations to include iterative or multiple-round stipulations or refinements could be promising. Moreover, assessing the game theoretic situations that firms and data gatherers confront in uncertain or chaotic regulative environments should also be instructive for understanding the important and vital notion of institutional trust.

ENDNOTE

1. For the purposes of this article, and in anticipation of the discussion of GDPR that follows, the terms "data controller," "firm," and "company" are sometimes used interchangeably and result from the attempt to compare the different consumer privacy protections in place in the EU and US, respectively.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Anonymous, A. (2013). Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. *Journal of Privacy and Confidentiality*, *4*(2). https://doi.org/10.29012/jpc.v4i2.623

Anscombe, F.J., & Aumann, R.J. (1963). A definition of subjective probability. *The Annals of Mathematical Statistics*, *34*(1), 199–205. https://doi.org/10.1214/aoms/1177704255

Barth, S., & de Jong, M.D.T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Binmore, K. (1994). *Game theory and the social contract, Volume 1: Playing fair*. Retrieved from https://www.proquest.com/books/game-theory-social-contract-volume-1-playing-fair/docview/60832919/se-2

Binmore, K.G. (2007). *Game theory: A very short introduction*. Oxford University Press.

Bloomberg Law. (2023, July 26). *Which States Have Consumer Data Privacy Laws? June 26, 2023*. Bloomberlaw.com. Retrieved from https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/

Breen, S., Ouazzane, K., & Patel, P. (2020). GDPR: Is your consent valid? *Business Information Review*, *37*(1), 19–24. https://doi.org/10.1177/0266382120903254

Calo, R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, *87*(3), 1027–72.

Ermakova, T., Krasnova, H., & Fabian, B. (2016). Exploring the impact of readability of privacy policies on users' trust. *Research Papers*, *20*. Retrieved from http://aisel.aisnet.org/ecis2016_rp/20

European Parliament and of the Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of April 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 (General Data Protection Regulation). *Official Journal of the European Union*, *L119*,1–88.

Fracassi, C., & Magnuson, W. (2021). Data Autonomy. *Vanderbilt Law Review*, *74*(2), 327–383.

Gal, M.S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, *16*(3), 349–391. https://doi.org/10.1093/joclec/nhaa012

Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *The International and Comparative Law Quarterly*, *71*(4), 799–830. https://doi.org/10.1017/S0020589322000355

Godinho de Matos, M., & Adjerid, I. (2022). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Science*, *68*(5), 3330–3378.

Ke, T.T., & Sudhir, K. (2022). Privacy rights and data security: GDPR and personal data markets. *Management Science*, *69*(8), 4363–4971. https://doi.org/10.1287/mnsc.2022.4614

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–34.

Kovářík, J., Levin, D., & Wang, T. (2016). Ellsberg paradox: Ambiguity and complexity aversions compared. *Journal of Risk and Uncertainty*, *52*(1), 47–64. https://doi.org/10.1007/s11166-016-9232-0

Maclean, A. (2009). *Autonomy, informed consent and medical law: A relational challenge.* Cambridge University Press.

Manson, N.C., & O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge University Press.

Martin, K. (2015, Fall). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, *34*, 210–227.

Menon, M. (2019). GDPR and data powered marketing: The beginning of a new paradigm. *Journal of Marketing Development and Competitiveness*, *13*(2), 73–84.

Milne, G.R., & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29.

Milne, G.R., Culnan, M.J., & Greene, H. (2006, Fall). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*, 238–49.

Muris, T.J. (2001, October 4). Protecting consumers' privacy: 2002 and beyond. In *Remarks at the FTC Privacy 2001 Conference*. Retrieved from https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.
Ohlhausen, M.K. (2014, Spring). Privacy challenges and opportunities: The role of the federal trade commission. *Journal of Public Policy & Marketing*, *33*, 4–9.
Peltier, J.W., Milne, G.R., Phelps, J.E., & Barrett, J.T. (2010). Teaching information privacy in marketing courses: Key educational issues for principles of marketing and elective marketing courses. *Journal of Marketing Education*, *32*(2), 224–246.
Peslak, A.R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, *59*(4), 327–45.
Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*, *41*(4), 746–768. https://doi.org/10.1287/mksc.2021.1339
Ross, D. (2016, Winter). Game Theory. In E. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Retrieved from https://plato.stanford.edu/archives/win2016/entries/game-theory/
Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at a glance. *Information Systems*, *106*, 101876. https://doi.org/10.1016/j.is.2021.101876
Schwalbe, U., & Walker, P. (2001). Zermelo and the early history of game theory. *Games and Economic Behavior*, *34*(1), 123–137.
Schweigert, V., & Geyer-Schulz, A. (2019). The impact of the general data protection regulation on the design and measurement of marketing activities: Introducing permission marketing and tracking for improved marketing & CRM compliance with legal requirements. *Journal of Marketing Development and Competitiveness*, *13*(4), 63–71.
Slepchuk, A.N., & Milne, G.R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, *31*, 89–93. https://doi.org/10.1016/j.copsyc.2019.08.007
Tamburri, D.A. (2020). Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, *91*, 101469. https://doi.org/10.1016/j.is.2019.101469
Tang, Z., Hu, Y., & Smith, M.D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, *24*(4), 153–173. https://doi.org/10.2753/MIS0742-1222240406
Thierer, A. (2013). A framework for benefit-cost analysis in digital privacy debates. *George Mason Law Review*, *20*(4), 1055–1105.
Urbany, J.E., Dickson, P.R., & Wilkie, W.L. (1989). Buyer uncertainty and information search. *The Journal of Consumer Research*, *16*(2), 208–215. https://doi.org/10.1086/209209
van Ooijen, I., & Vrabec, H.U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7
Vila, T., Greenstadt, R., & Molnar, D. (2003). Why we can't be bothered to read privacy policies models of Privacy Economics as a Lemons Market. In *Proceedings ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce, Association for Computing Machinery*, pp. 403–407. https://doi.org/10.1145/948005.948057
Voss, W.G., & Houser, K.A. (2019). Personal data and the GDPR: Providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287–344. https://doi.org/10.1111/ablj.12139
Walker, K.L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, *35*, 144–158.
Warner, R. (2020). Notice and choice must go: The collective control alternative. *SMU Science and Technology Law Review*, *23*(2), 173.
Zaeem, R.N., & Barber, K.S. (2021). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems*, *12*(1), 1–20. https://doi.org/10.1145/3389685