Abstract. Consider a mechanism designer who implements a choice rule through a dynamic protocol, gradually learning agents’ private information through yes-or-no questions addressed to one agent at a time. A protocol is contextually private for a choice rule if the designer learns only the subsets of private information needed to determine the outcome. While the serial dictatorship and the first-price auction have contextually private implementations, the second-price auction does not, nor does any stable matching rule. When the designer can additionally ask about the number of agents whose private information satisfies a certain property, the second-price auction, the uniform \( k \)th price auction, and the Walrasian double auction have contextually private tâtonnement implementations.

**Keywords:** Mechanism design, privacy, auctions, matching.

1. **INTRODUCTION**

In mechanism design, agents weigh the expected benefits of revealing their private information against potential costs. The designer’s role is to create the right allocative incentives for agents to voluntarily and truthfully reveal their private information. However, it has long been recognized that even if the designer provides the right allocative incentives, agents may still be reluctant to reveal their private information (Vickrey, 1961). Agents may worry that their private information will be used against them in subsequent interactions with the designer or third parties (Rothkopf et al., 1990), or that it may enable the designer to stray from a stated plan (Akbarpour and Li, 2020).

These privacy concerns are not abstract. Consider the following allegation from a recent lawsuit against Google, which takes aim at the company’s second-price auctions for advertising:

> Google induced advertisers to bid their true value, only to override pre-set AdX floors and use advertisers’ true value bids against them... Google abused advertisers’ trust and secretly... generated unique and custom per-buyer floors depending on what a buyer had bid in the past.

State of Texas et al. v. Google, 2022

In short, the plaintiffs alleged that Google used advertisers’ losing bids in prior auctions to set personalized reserve prices in future auctions, thereby using information against the participants who supplied it. The allegation highlights a class of situations that may be particularly worrisome from a privacy perspective: those in which agents are asked to reveal private information which the designer does not actually need in order to carry out its stated plan. A low bidder in a strategyproof auction reveals her exact willingness to pay even though the result of the auction would have been the same if the designer only knew that her type fell below a threshold. A student with a low priority score at desirable schools reveals her entire preference...
ranking even though she would have ended up at a low priority school irrespective of her preference ranking. In such settings, the designer learns more than is needed—some agents seem to give up their privacy for no reason.

In this paper, we study dynamic implementations of mechanisms in which the only information that is learned by the designer is essential to the designer’s ability to compute the outcome of a mechanism they committed to. These dynamic implementations allow the designer to learn agents’ private information in a minimal way, ruling out type profiles until the designer knows exactly what is needed to compute the outcome, and nothing more. We call the mechanisms that have such implementations contextually private—the designer’s access of agents’ private information is justified by the market context.

We focus on a restricted class of dynamic implementations that resemble extensive-form games of perfect recall. This restriction rules out a wide range of sophisticated cryptographic solutions that could, in principle, completely solve mechanism design’s privacy problem. But in some environments, sophisticated cryptography may be excessively costly in terms of time, money or computational power. In addition, sophisticated cryptographic mechanisms require sophisticated participants—if participants don’t understand how their information is kept private, their privacy concerns may not be alleviated. Furthermore, even if possible, some sophisticated solutions may be wasteful—in one of the earliest large-scale uses of secure multi-party computation, a double auction with sugar beet farmers in Denmark, designers wondered “if the full power of multiparty computation was actually needed,” or if a simpler implementation guided by a weaker privacy criterion may have sufficed.

To formalize the restricted process through which designers learn subsets of agents’ private information, we define protocols. The protocols we study are made up of queries, and allow us to formulate processes that go beyond the possibilities for information revelation in extensive-form games. Queries can be interpreted from a communication perspective or an access perspective: they can represent a live query to an agent (“communication”) or a query of a secure database that the designer can only access through such queries (“access”). At the start of a protocol, the designer knows that the true type profile of agents lies in the type space. Each query narrows down the set in which the true type profile lies.

A query is a direct question about one agent’s type, as if the agent is being called to play in an extensive-form game, or as if the designer is querying an agent-identified entry in a database. We call protocols made up of such queries sequential elicitation protocols. In contrast to more sophisticated cryptographic techniques, the technology required to prove exactly what has been learned about agent $i$ through a sequential elicitation protocol is simple. From the communication perspective, the agent need only recall her experience of game play to know what the designer learned about her. From the access perspective, all that is needed is a tamper-evident technology—in a digital implementation, a trusted file-monitoring software such as SolarWinds or Tripwire would be enough. In an analog implementation, agents could submit subsets of their private information in sealed envelopes, and the designer could send back the

---

2 Secure multi-party computation, zero-knowledge proofs and homomorphic encryption can, under intractability assumptions, block all information transmission to the designer (Alvarez and Nojoumian, 2020).

3 For instance, Google’s auctions run in a fraction of a second—making any computational overhead, such as the overhead incurred through high-tech cryptographic calculations, particularly costly (Pachilakis et al., 2019).

4 A recent survey shows that only 61% of WhatsApp’s users believe the company’s claim that their messages are end-to-end encrypted (Alawadhi, 2021).

5 We treat the communication and access perspectives as equivalent throughout this paper. Clearly, the communication and access perspectives raise different strategic considerations which we discuss in subsection 2.2.
sealed envelopes at the conclusion of the game.\textsuperscript{6} To illustrate contextual privacy, we turn to an introductory example.

1.1. Introductory Example

Suppose there are two agents, 1 and 2, and two objects, $A$ and $B$. The designer chooses a choice rule and a communication protocol to allocate the objects to the agents. An agent’s private information is her preferred object, $A$ or $B$, which we call her “type”. At the start of the protocol, the designer knows that the true type lies in the type space $\{A, B\}^2$. For this type space, we visualize a protocol as a directed rooted tree, labelled by the sets of type profiles that the designer has not yet ruled out. We can visualize the nodes of this tree as $2 \times 2$ boxes (see Figure 1). In each box, the rows represent possible types for agent 1 and the columns represent possible types for agent 2. The shaded boxes in Figure 1 represent type profiles that the designer has ruled out with its queries.

An example of a query, shown in Figure 1 is: “Is agent 1’s type $A$?” With this query, the designer learns either that agent 1’s type is $A$ or that it is $B$. These two possibilities correspond to the left and right child, respectively. The left arrow points to a refined type space in which the bottom row is ruled out, while the right arrow points to a refined type space in which the top row is ruled out.

A protocol is contextually private for a choice rule $\phi$ if each piece of information revealed through the protocol is necessary for determining the outcome of the choice rule. More precisely, a protocol is contextually private if the designer can only distinguish between possible types of agents in the event that the two types lead to different outcomes, holding other agent types fixed. A choice rule is contextually privately implementable if there is a contextually private protocol that implements it.

To see how choice rules fail to be contextually private, suppose the designer wants to implement a simple efficient choice rule $\phi^{\text{fair}}$: give each agent their preferred object and break one of the possible ties in agent 1’s favor, and the other tie in agent 2’s favor. More formally, let $(i, x)$

\textsuperscript{6}Tamper-evident technologies for protecting communications have existed for millennia, which confirms their technological primitiveness. Ancient Romans sealed letters with unique insignia pressed into wax seals so that others without their signet rings could not secretly reseal the letter. Since at least the 13th century, writers of secure messages on paper have sealed their messages through an intricate series folds and cuts in a practice known as letterlocking (Cain, 2018).
represent an allocation in which agent $i \in \{1, 2\}$ is allocated object $x \in \{A, B\}$. The choice rule $\phi_{\text{fair}}$ is then

$$
\phi_{\text{fair}}(\theta) = \begin{cases} 
(1, A), (2, B) & \text{if } \theta \in \{(A, B), (A, A), (B, B)\} \\
(1, B), (2, A) & \text{if } \theta = (B, A).
\end{cases}
$$

The designer cannot implement $\phi_{\text{fair}}$ with a contextually private protocol. To see this, consider again the query that asks “Is agent 1’s type A?” (as shown in Figure 1). If the answer is “yes” (left arrow), then the designer knows that the true type profile $\theta$ is either $(A, A)$ or $(A, B)$, and for either of these types, the outcome under $\phi_{\text{fair}}$ is $(1, A)$ and $(2, B)$. However, if the answer is “no” (right arrow) then the designer learns that the true type is either $(B, A)$ or $(B, B)$. In this event, the designer does not have enough information to compute the choice rule, because the two possible type profiles—$(B, A)$ and $(A, B)$—result in different outcomes under $\phi_{\text{fair}}$.

So, in order to compute the choice rule, the designer must pose another query: “Is agent 2’s type A?” This second query, combined with the first, allows the designer to distinguish between type profiles $(B, A)$ and $(B, B)$ and therefore compute the choice rule. But, this choice rule violates contextual privacy for agent 2. To see this, suppose the true type profile is $(B, A)$. In this case, agent 1 gets object $A$ and agent 2 gets object $B$, and the designer knows that agent 2’s type is $A$ and not $B$. But, notice that holding agent 1’s type fixed at $A$, it did not matter whether agent 2 had type $A$ or $B$, the social outcome would have been $(1, A)$ and $(2, B)$ regardless. The designer did not need to know that agent 2 had type $A$ and not $B$. So, $\phi_{\text{fair}}$ is not contextually private. As we will see, contextual privacy is a demanding criterion, at least if only sequential elicitation protocols are admitted.

### 1.2. Overview

After articulating our formal framework in Section 2, we present the main characterization of contextual privacy in Section 3. We show that the descending auction is a contextually private implementation of the first-price choice rule, and that the serial dictatorship is contextually private. In addition to these positive results, we present a host of negative results in domains with and without transfers: neither the second-price auction nor the Walrasian double auction is contextually private; there is no stable matching rule that is contextually private; and there is no efficient and individually rational house assignment rule.

Next, in Section 4, we expand the designer’s toolkit and ask whether the set of contextually private choice rules expands accordingly. We first define tâtonnement protocols to be protocols in which, roughly speaking, a “price-finding” phase is followed by a “price-taking” phase. After proving that tâtonnement protocols are contextually private, we ask what kind of queries are required to implement tâtonnement protocols. In particular, we ask what the designer can do with a simple kind of query we call a count query: a count query allows the designer to ask for the number of agents whose types satisfy a particular property, without learning which agents have this property. We find that when the designer can use such queries, the second price auction, and the Walrasian double auction have tâtonnement implementations, and are thus contextually private.

Section 5 explores two modifications of contextual privacy. With these extensions, we illustrate which of our results are robust to alternative specifications of contextual privacy. These extensions are also valuable from a theoretical perspective. They highlight connections to other concepts such as non-bossiness (Satterthwaite and Sonnenschein, 1981, Pycia and Raghavan, 2022).
A discussion of related literature in Section 6 follows the extensions. We draw out comparisons between contextual privacy and unconditional winner privacy (Brandt and Sandholm, 2008)—the concept from decentralized computing to which contextual privacy owes the deepest intellectual debt—as well as credibility (Akbarpour and Li, 2020), a concept which is motivated by similar concerns. We also discuss differential privacy (Dwork, 2006)—an influential concept in computer science that has been incorporated into mechanism design (see Pai and Roth (2013) for a review). Section 7 concludes.

Omitted proofs are found in the appendix. Online appendices A, B and C contain additional discussion and statements.

2. MODEL

Consider a set $\mathcal{N} = \{1, 2, \ldots, n\}$ of agents with private types $\theta_i \in \Theta$. We denote by $\theta = (\theta_1, \theta_2, \ldots, \theta_n) \in \Theta = \Theta^n$ a profile of agents’ types. Agents have utility functions $u$ over outcomes in $\mathcal{X}$ which depend on their private types, with $u_i : \Theta \times \mathcal{X} \to \mathbb{R}$. The designer has a social choice function $\phi : \Theta \to \mathcal{X}$ that assigns outcomes in $\mathcal{X}$ based on type profiles $\theta \in \Theta$ (we use bold characters to refer to type profiles). All primitives of the model besides the true type profile $\theta$ are common knowledge.

2.1. Protocols

The designer chooses a protocol to implement the choice rule. A protocol is a process through which the designer learns agents’ private information. This article considers deterministic rules and protocols. Formally, protocols are generalizations of extensive-form game trees with perfect recall.

**Definition**—Protocol: A protocol $P$ is a directed rooted tree with vertices $V$ and edges $E$. Each vertex is labelled with a non-empty subset $\Theta_v \subseteq \Theta$, the type profiles possible at $v$, and each edge is labeled with $i \in \mathcal{N}$. The root vertex of $(V, E)$ is labelled with the full joint type space $\Theta$. The labels of children $w$ form a partition of the label of the parent node $\Theta_v$, i.e.

$$\Theta_v = \bigcup_{w : (v, w) \in E} \Theta_w.$$ 

We call nodes with zero out-degree terminal and label them $z$. We call all other nodes interior. Interior nodes can be understood as questions about the true type profile—different outgoing edges lead to different new information that the principal learns about the true type profile $\theta$. For this reason, we will refer to interior nodes also as queries. This definition is illustrated on the left in Figure 2.

We say that a protocol $P$ implements a social choice rule $\phi$ if $P$ yields sufficient information to compute the choice rule: For any terminal node $z$, any distinct type profiles that remain possible at at node terminal node $z$ (i.e. $\theta, \theta' \in \Theta_z$) lead to the same outcome under $\phi$, i.e.

$$\phi(\theta) = \phi(\theta').$$

---

\(^7\)We restrict attention to deterministic protocols for two reasons. First, it is not immediately clear how to define contextual privacy for randomized rules—there are at least two natural extensions of contextual privacy, depending on whether randomization with public or with private sources of randomness is allowed. Second, there are many contrived stochastic choice rules that are trivially contextually private. For instance, a rule that places $\epsilon$ probability on outcome that uses each agent $i$’s exact type is trivially contextually private.
In other words, a protocol $P$ implements the choice rule $\phi$ if $\phi$ is measurable with respect to the partition induced by terminal nodes of $P$. When $P$ implements $\phi$, we sometimes say $P$ is a protocol for $\phi$.

For any two type profiles $\theta, \theta'$ there is a node $v$ such that for two children of $v$, labelled $w$ and $w'$, it is the case that $\theta \in \Theta_w$ while $\theta' \in \Theta_{w'}$. We say that $\theta, \theta'$ are separated at $v$ or that their earliest point of departure is $v$.

The main definition of this article is a property of protocols for a given choice rule $\phi$.

**DEFINITION—Contextually Private Protocol:** A protocol $P = (V,E)$ for a social choice function $\phi$ is **contextually private** if for all terminal nodes $z, z' \in Z_P$ and all type profiles $(\theta_i, \theta_{-i}) \in \Theta_z, (\theta'_i, \theta_{-i}) \in \Theta_{z'}$,

$$\phi(\theta_i, \theta_{-i}) \neq \phi(\theta'_i, \theta_{-i}).$$  \hspace{1cm} (1)

Roughly, a protocol is contextually private if for all agents $i$ and all partial type profiles for agents except $i$, the designer can distinguish some $\theta_i$ from some $\theta'_i$ at the conclusion of the protocol if and only if $\theta_i$ and $\theta'_i$ result in different outcomes under $\phi$. This criterion captures the idea that there must be a reason that the designer needed to know whether agent $i$ had type $\theta_i$ and not $\theta'_i$, holding other agents’ types fixed at $\theta_{-i}$. That reason, in particular, is that without distinguishing $\theta_i$ from $\theta'_i$, the designer could not have determined the overall allocation. This definition is illustrated on the right in Figure 2. The definition of contextually private protocols induces an implementation notion.

**DEFINITION—Contextually Private Implementation:** A choice rule $\phi$ is **contextually privately implementable under a class of protocols $\mathcal{P}$** if there exists a protocol $P \in \mathcal{P}$ for $\phi$ that is contextually private.

To ease diction, we sometimes say that a choice rule is **contextually private** when it is contextually privately implementable. Contextually private implementation (or **contextual privacy**) is a property of a choice rule $\phi$ in a given environment characterized by protocols in class $\mathcal{P}$.

Notice that contextual privacy depends both on the choice rule $\phi$ and the set of admissible protocols $\mathcal{P}$. As noted in the introduction, if the designer had access to arbitrary cryptographic protocols, contextual privacy (and indeed much stronger privacy criteria) would be easy to satisfy. The key results in this article apply in settings where the set of admissible protocols is

---

**Table 1. Notation for Protocols**

| Name              | Sets            | Representative Element |
|-------------------|-----------------|------------------------|
| Agents            | $\{1, \ldots, n\}$ | $i$                    |
| Agent types       | $\Theta$        | $\theta$               |
| Type profiles     | $\Theta = \Theta^n$ | $\theta$               |
| Protocols         | $P = (V,E)$     | $v, w$                 |
| Nodes             | $V$             | $v, w$                 |
| Queries           | $E$             | $e = (v, w)$           |
| Terminal nodes of protocol $P$ | $Z_P$ | $z$ |
| Type profiles possible at node $v$ | $\Theta_v$ | $\theta_v$ |
| Projection of $\Theta$ onto component $i$ | $\Theta_i$ | $\theta_{[k]}$ |

---
severely restricted, for example only includes extensive-form games of perfect recall, in which one agent at a time is asked a yes-or-no question about her type. These are protocols where all queries are individual elicitation queries.

**Definition—Individual Elicitation Query:** Let $P = (V, E)$ be a protocol. A query for $\Theta_v$ is an individual elicitation query if there is an agent $i$ such that the query can be determined using information on $\theta_i$ only, i.e. for all $(v, w) \in E$, $(\theta_i, \theta_{-i}) \neq (\theta_i', \theta_{-i}')$, either $(\theta_i, \theta_{-i}), (\theta_i, \theta_{-i})' \in \Theta_w$ or $(\theta_i, \theta_{-i}), (\theta_i, \theta_{-i})' \notin \Theta_w$.

**Definition—Sequential Elicitation Protocol:** A protocol $P$ is a sequential elicitation protocol if all queries $(v, w) \in E$ are individual elicitation queries.

An individual elicitation query learns something about one agent at a time. For example, in an auction setting, an individual elicitation query could ask an agent $i$ whether their bid is above or below some value $x$. In an assignment setting, an individual elicitation query can ask agent $i$ whether they prefer item $A$ to item $B$.

The formalism outlined here is able to accommodate more general queries, which, as we show, allow to overcome some of the impossibility results we show for sequential elicitation queries. We will consider queries about the number of agents whose type satisfies a particular property, without learning the identity of the agents. We call these queries count queries.

**Definition—Count query:** A query for node $v$ is a count query if there is a set $\hat{\Theta}_v \subseteq \Theta$ such that for $(v, w) \in E$, for some $A \subseteq \{1, 2, \ldots, n\}$,

$$\Theta_w = \{\theta \in \Theta_v : |\{i \in N : \theta_i \in \hat{\Theta}_v\}| \in A\}.$$ 

A count query asks for the number of agents whose type lies in a certain subset of the type space. For example, in an auction setting, a count query could ask how many agents have a bid above some value $x$. In a double auction, a query could ask whether the market clears at a given price $p$. In an assignment setting, a count query can ask how many agents prefer item $A$ to item $B$. Whereas an individual elicitation query returns a yes-or-no answer to the question “Is agent $i$’s type in subset $\hat{\Theta}$?”, a count query gets an answer depending on how many agents have a type that lies in subset $\hat{\Theta}$.
Section 3 presents our main results, which characterize contextually private mechanisms when only sequential elicitation protocols are available. Then, in Section 4, we add count queries to the designer’s toolkit, and investigate how this addition expands the set of contextually private choice rules.

2.2. Incentives

In this paper, we deal only with “direct” mechanisms, in the sense that each mechanism we study is one in which agents are queried about their private information (“types”). Often, studying the implementability of such mechanisms is without loss of generality, because of the revelation principle. The revelation principle states that if a choice rule can be implemented by an arbitrary mechanism (i.e. there is a mechanism which has the outcome of the choice rule as an equilibrium outcome) then that choice rule can be implemented by a direct incentive-compatible mechanism (i.e. a direct incentive-compatible mechanism which has the outcome of the choice rule as an equilibrium outcome).

Under restrictions on the amount of information the designer may elicit, the revelation principle need not hold, depending on the interpretation of protocols. Under the data access perspective introduced in Section 1, agents submit their type reports using some pre-specified secure technology, e.g., tamper-evident envelopes. The protocol then describes how the designer accesses the pre-collected information. Their incentives are the same as they would be in a one-shot normal-form game in which they revealed all of their private information in a single report (as is standard in mechanism design).

With the communication interpretation, agents answer queries dynamically, and a protocol defines an extensive-form game. This, in general, alters agents’ truth-telling incentives, even for strategy-proof choice rules. It is beyond the scope of the current paper to study agents’ incentives under the communication interpretation.

We note that all choice rules we consider in this article have Bayes-Nash equilibria with bijective strategies. (For example, a first-price auction with two players of independently uniformly distributed mechanisms has a symmetric Bayes-Nash equilibrium in bids $\frac{1}{2}\theta_i$, $i = 1, 2$.) So, in games we consider, protocols that elicit information about types can be thought of equivalently as protocols that elicit information about actions.

3. THE DEMANDS OF CONTEXTUAL PRIVACY UNDER SEQUENTIAL ELICITATION

When the designer is restricted to protocols that resemble extensive-form games, contextual privacy puts severe restrictions on implementation. Most of the results in this section are negative—they cover choice rules and classes of choice rules that are not contextually private. However, there are two notable positive results. In the domain of mechanisms with transfers, the first-price auction rule is contextually private with a descending or Dutch auction protocol. In the domain of mechanisms without transfers, the serial dictatorship is contextually private.

We start this section with a characterization of contextually private mechanisms, and a useful necessary condition. The characterization will make use of a particular equivalence relation on types, which we call inseparability. Roughly, two types for an agent $i$ are inseparable if the designer cannot distinguish between them without violating contextual privacy.

Our concept of inseparability parallels the concept of forbidden matrices used in the work on decentralized computation Chor and Kushilevitz (1989), Chor et al. (1994). Our statement is more general in that it captures agents more than 2 agents.
**Definition**—Inseparable Types: For a social choice function $\phi$, call two types $\theta_i, \theta'_i$ for an agent $i$ **directly inseparable** on $\Theta'$, denoted $\theta_i \sim_{i,\phi,\Theta'} \theta'_i$ if there exists $\theta_{-i}$ such that $(\theta_i, \theta_{-i}), (\theta'_i, \theta_{-i}) \in \Theta'$, and

$$\phi(\theta_i, \theta_{-i}) = \phi(\theta'_i, \theta_{-i}).$$

Denote the transitive closure of $\sim'_{i,\phi,\Theta'}$ by $\sim_{i,\phi,\Theta'}$. If $\theta_i \sim_{i,\phi,\Theta'} \theta'_i$, call $\theta_i$ and $\theta'_i$ **inseparable** for $i$. We denote equivalence classes under $\sim_{i,\phi,\Theta'}$ by $[\theta]_{i,\phi,\Theta'}$.

We can view inseparability as a necessary condition for contextual privacy when $\phi$ is evaluated on a subset of type profiles $\Theta'$. We will denote the evaluation of $\phi$ on a restricted set of type profiles $\Theta$ as $\phi|_{\Theta}$. Assume that the designer arrives at an interior node $v$ such that $\Theta_v = \Theta'$. Then, a query to agent $i$ that separates $\theta_i$ and $\theta'_i$ leads to a violation of contextual privacy, as $\phi(\theta_i, \theta_{-i}) = \phi(\theta'_i, \theta_{-i})$. When the designer learns something that “separates” inseparable types, it learns something that it didn’t need to know.

As inseparability will be important for the central characterization of the paper, we build further intuition for this definition. See Figure 3 for an illustration of inseparable types. The $3 \times 3$ grid represents a subset of the type space in a setting where there are two agents ($n = 2$). The shaded regions of the grid represent type profiles for which the outcome under $\phi$ is a particular outcome $x \in \mathcal{X}$. Regions of the grid that are not shaded in lead to arbitrary outcomes under $\phi$. On $\Theta'$, all of agent 2’s types are inseparable. To see this, note that $\theta_1$ and $\theta_2$ are directly inseparable—they lead to the same outcome $x$ when agent 1’s type is fixed at $\theta_3$. Furthermore, for agent 2, $\theta_2$ and $\theta_3$ are directly inseparable, since they lead to the same outcome $x$ when agent 1’s type is fixed at $\theta_1$. So, since inseparability is transitive, $\theta_1, \theta_2$ and $\theta_3$ are all inseparable for agent 2.

In short, when a choice rule $\phi$ requires separating inseparable types, contextual privacy is violated. Note that a particular protocol for $\phi$ may not in fact arrive at an interior node such that $\Theta_v = \Theta'$. However, the fact that some product set $\Theta'$ exists where all contained types are inseparable and $\phi$ is nonconstant already implies a violation of contextual privacy, as the following characterization shows.

**Proposition 1**—Characterization of Contextually Private Choice Functions Under Sequential Elicitation Protocols: A choice function $\phi$ is contextually private if and only if there is no product set $\Theta'$ such that $\phi|_{\Theta'}$ is non-constant and for all agents $i$ and all $\theta_i, \theta'_i \in \Theta'_i$, $\theta_i$ and $\theta'_i$ are inseparable.

Note that the restriction to product sets is natural: For any sequential elicitation protocol, it needs to be that all spaces of type profiles $\Theta_v$ are products, i.e. $\Theta_v = \times_{i=1}^n \Theta_i$. 

**Figure 3.**—Illustration of Inseparable Types with $n = 2$, $\Theta' = \{\theta_1, \theta_2, \theta_3\}^2$. Shaded regions represent outcome $x$ under $\phi$. For agent 1, $\theta_3 \sim_{1,\phi,\Theta', \theta_1}$. For agent 2, $\theta_1 \sim_{2,\phi,\Theta'}$, $\theta_2 \sim_{2,\phi,\Theta'}$, $\theta_3$. 

\[\text{Agent 1 Type} \]
\[\theta_1 \quad \theta_2 \quad \theta_3\]
\[\text{Agent 2 Type} \]
\[\theta_1 \quad \theta_2 \quad \theta_3\]
PROOF: We first consider necessity. Assume for contradiction that there is a contextually private protocol $P$ for the choice function $\phi$ and that there is a product set $\Theta'$ such that all types are inseparable under $\Theta'$ and $\phi$ is non-constant on this set.

As $\phi$ is nonconstant on $\Theta'$, the protocol must make a query separating type profiles $(\theta, \theta_{-i})$ and $(\theta', \theta_{-i})$ for $\theta \neq \theta_{-i}, \theta'$ for some agent $i$. Consider the earliest such query in the precedence order on $P$.

By the choice of $v$ and $\theta \sim_i \theta, \theta' \theta'$, there must be a chain $\theta_1, \theta_2, \ldots, \theta_k$ such that $\theta_1 = \theta$ and $\theta_k = \theta'$ and

$$\theta_1 \sim_i \theta, \theta' \theta_2 \sim_i \theta, \theta' \cdots \sim_i \theta, \theta' \theta_k.$$

That is, there is a chain of direct inseparability from $\theta$ to $\theta'$. As $\theta$ and $\theta'$ are separated at $v$, there must be $l = 1, 2, \ldots, k - 1$ such that $\theta^l$ is separated from $\theta^{l+1}$ at $v$. As a property of sequential elicitation protocols, for any $\theta_{-i}$ such that $(\theta^l, \theta_{-i}), (\theta^{l+1}, \theta_{-i}) \in \Theta' \subseteq \Theta_v$, $(\theta^{l+1}, \theta_{-i})$ and $(\theta^l, \theta_{-i})$ lead to distinct terminal nodes. By direct inseparability, there is $\theta_{-i}$ such that $(\theta^l, \theta_{-i}), (\theta^{l+1}, \theta_{-i}) \in \Theta'$ and $\phi(\theta^l, \theta_{-i}) = \phi(\theta^{l+1}, \theta_{-i})$. Together, these two observations yield a contradiction to contextual privacy of $P$.

Now consider sufficiency. We define a contextually private protocol inductively. Throughout the induction, the following holds:

For any terminal nodes $w, w'$ whose earliest point of departure in $P$ is $v$, there are no $(\theta_1, \theta_{-i}) \in \Theta_v$ and $(\theta'_1, \theta_{-i}) \in \Theta_v$ such that $\phi(\theta_1, \theta_{-i}) = \phi(\theta'_1, \theta_{-i})$.\hspace{1cm} (2)

Note that a protocol that satisfies (2) at all internal nodes is contextually private. We prove the statement by induction over the tree $P$.

Assume a protocol has been constructed until query $v$ associated to type set $\Theta_v \subseteq \Theta$. If $\phi$ is constant on the remaining set, the node is terminal, and the outcome of the social choice function can be determined.

Otherwise, because there is no restriction to a product set $\Theta'$ under which all types are inseparable, there are types $\theta, \theta'$ that are separable under $\Theta_v$ for agent $i$. Consider the binary query that separates the equivalence class of $\theta$, $[\theta]_{i, \phi, \Theta_v}$, from its complement $\Theta_v \setminus [\theta]_{i, \phi, \Theta_v}$, which is non-empty as it contains at least $\theta'$. By definition of $\sim$, for any $\theta_{-i}$,

$$\phi(\tilde{\theta}_i, \theta_{-i}) \neq \phi(\tilde{\theta}'_i, \theta_{-i}),\hspace{1cm} (3)$$

implying that (2) continues to hold. By induction, it holds at all internal nodes. Q.E.D.

The full characterization is often not necessary to disprove contextually private implementability. A more minimal necessary condition, which is a corollary, dramatically simplifies impossibility results.

COROLLARY 1—Corners Lemma (compare Chor and Kushilevitz (1989)): Let $\phi$ be contextually private under sequential elicitation protocols. Then, for any fixed $\theta_{-i, -j} \in \Theta_{-i, -j}$, for all types $\theta_i, \theta'_i, \theta_j, \theta'_j \in \Theta$,

$$\phi(\theta_i, \theta_{j, \theta_{-i, -j}}) = \phi(\theta'_i, \theta_j, \theta_{-i, -j}) = \phi(\theta_i, \theta'_j, \theta_{-i, -j}) = x \implies \phi(\theta'_i, \theta'_j, \theta_{-i, -j}) = x.\hspace{1cm} (4)$$

PROOF: Consider the product set $\Theta' = \{\theta_i, \theta'_i\} \times \{\theta_j, \theta'_j\} \times \times_{k \in \mathcal{N} \setminus \{i, j\}} \{\theta_k\}$. By assumption, $\theta_i$ and $\theta'_i$ resp. $\theta_j$ and $\theta'_j$ are directly inseparable, and $\phi$ is non-constant on $\Theta'$. Hence, by Proposition 1, $\phi$ is not contextually privately implementable. Q.E.D.
The Corners Lemma can be seen as a minimal (in terms of number of agents and types) counterexample to contextual privacy. It is best understood graphically. Hold fixed the types of all agents who are neither agent $i$ nor agent $j$ (i.e. hold $\theta_{-i,-j}$ fixed). Look only at the $|\Theta| \times |\Theta|$ square that represents the types of any two agents $i$ and $j$. A $2 \times 2$ sub-square is shown in Figure 1. If a choice rule $\phi$ is contextually private under sequential elicitation protocols, then it must be the case that, when three of the four quadrants in any such square result in outcome $x$, the fourth quadrant also results in $x$.

### 3.1. Limits of Contextual Privacy in Assignment Domains

In the assignment domain, we fix a set $C$ of objects. The set of outcomes is $\mathcal{X} = 2^{N \times C}$.

In the standard object assignment setting, agents may receive at most one object, and agents have ordinal preferences over objects, which are private information. So agents’ types $\theta \in \Theta$ are preference orders of $C$ where $\succ_i$ reference to agent $i$’s preference ordering. A choice rule $\phi$ is efficient if there is no outcome $x$ such that $x \succeq_i \phi_i(\theta)$ for all agents $i$ and $x \succ_j \phi_j(\theta)$ for some agent $j$.

Let $A \subseteq N \times C$ be an outcome. A partial assignment $N(A)$ is the set of agents who have an assigned object in $A$, i.e. $N(A) = \{i \in N : \exists c \in C : (i, c) \in A\} \subseteq N$. If $N(A) = N$, we call $A$ complete. For a partial assignment $A$, denote $A(i)$ the (at most one) object assigned to agent $i$.

The remaining objects $R(A)$ are the objects that do not have an assigned agent in $A$, i.e. $R(A) := \{c \in C : \nexists i \in N : (i, c) \in A\}$.

We first study serial dictatorship mechanisms, in which agents are sequentially asked to choose one of the remaining objects. To define the serial dictatorship protocol in our notation, we characterize the nodes and edges of the rooted tree. Fix the permutation $\pi : N \rightarrow N$ of agents that defines the priority order of the serial dictatorship. The serial dictatorship protocol with respect to $\pi$ has as nodes all partial assignments to agents in $N_1^\pi := \{\pi(i') : 1 \leq i' \leq i\}$ for any $i \in N$. Edges are between partial assignments $A, A'$ such that exactly agents $N_{\pi(i)}^\pi$ resp. $N_{\pi(i)+1}^\pi$ are assigned an object, $N(A_i) = N_i^\pi$ and $N(A_{i+1}) = N_{i+1}^\pi$, and $\pi(1), \pi(2), \ldots, \pi(i)$ are assigned the same objects. We define sets of type profiles associated to each node recursively. For an edge $(A, A')$,

$$\Theta^{A'} = \Theta^A \cap \left\{ \theta \in \Theta : \max_{\Theta_{\pi(i)}} R(A) = A'(\pi(i + 1)) \right\}.$$  

Here, $R(i)$ is the set of remaining objects when it is agent $i$’s turn in the partial order; $\max_{\Theta_{\pi(i)}} R(i)$ is the most preferred element of $R(i)$ with respect to the strict order $\theta_{\pi(i)}$. If a node is reached that is a complete assignment, the protocol ends, and the complete assignment is implemented.

**Proposition 2:** Serial dictatorships are contextually private under sequential elicitation.

The above protocol for the serial dictatorship satisfies even stronger versions of contextual privacy. For any $\theta, \theta'$ in distinct terminal nodes of the protocol, $\phi(\theta) = \phi(\theta')$. The reason for this is that at an earliest point of departure, the assignment to an agent is different, and any actions by later agents will lead to different outcomes. Such group-contextually private mechanism may be formulated as restricting the set of outcomes. Additionally, if $\theta_i, \theta'_i$ are such that for some $\theta_{-i}, (\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ are in distinct terminal nodes, it holds that $\phi_i(\theta_i, \theta_{-i}) \neq \phi'_i(\theta_i, \theta_{-i})$, serial dictatorships are individually contextually private. We discuss both of these strengthenings in Section 5.
and a type $\theta$ they prefer their own endowment to all other objects, i.e. other’s. When the profile is rational, efficient and contextually private choice rule under sequential elicitation.

Our characterizations add to a long list of special properties of the serial dictatorship. It is strategyproof and efficient, uniquely obviously strategyproof and efficient Pycia and Troyan (2021), and uniquely strategyproof, efficient, non-bossy and deterministic Bade (2020).

In the case of only two agents, serial dictatorship is the unique contextually private and efficient mechanism, as the following example shows.

**EXAMPLE**—Contextual Privacy and Serial Dictatorships, $n = 2$: Consider again the example from the introduction in Figure 1. There are two agents $\mathcal{N} = \{1, 2\}$, each of which is allocated an object $A$ or $B$. The two possible outcomes are $x = \{(1, A), (2, B)\}$ and $x' = \{(1, B), (2, A)\}$.

Table II shows possible assignments under efficiency. In the upper right table cell, efficiency requires that the outcome is $x$. In the lower left cell, efficiency requires that the outcome is $x'$. In the top left and bottom right cell, where both agents have the same type, efficiency allows either $x$ or $x'$.

Four different assignments remain. The first two assignments contain a Corner in the sense of Corollary 1, hence are not contextually private. The other two are Serial Dictatorships corresponding to the agent orderings $\pi(1) = 1, \pi(2) = 2$ resp. $\pi(1) = 2, \pi(2) = 1$.

As soon as, compared to serial dictatorship, more complexity in the form of endowments or object-specific priority scores is introduced, standard market design desiderata become incompatible with contextual privacy under sequential elicitation.

Consider first the house assignment problem Shapley and Scarf (1974). All agents are initially endowed with an object from $C$. Denote the initial assignment by an injective function $e: \mathcal{N} \rightarrow C$, where $e(i) \in C$ refers to agent $i$’s initial endowment. For our result it will be irrelevant whether the endowments are private information or known to the designer. We call a choice rule $\phi$ individually rational if for all $i \in \mathcal{N}$

$$\phi_i(\theta) \succeq_i e(i).$$

**PROPOSITION 3**: Assume agents have initial endowments $e(i)$. Then there is no individually rational, efficient and contextually private choice rule under sequential elicitation.

**PROOF**: The proof uses the Corners Lemma. Consider two agents $i$ and $j$ and two possible preference profiles for each agent. For agent $i$, consider a type $\theta_i$ which contains $e(i) \succ_i e(j)$, and a type $\theta'_i$ which contains $e(j) \succ_i e(i)$. For agent $j$, consider $\theta_j$ which contains $e(j) \succ_j e(i)$, and a type $\theta'_j$ which contains $e(i) \succ_j e(i)$. Hold fixed all other types $\theta_{-i,-j}$, to be such that they prefer their own endowment to all other objects, i.e. $\theta_{-i,-j} = \{\theta \in \Theta^{n-2}: e(k) \succeq_k c\}$ for all $c \in C \setminus \{e(k)\}$.

When the type profile is $(\theta_i, \theta_j, \theta_{-i,-j})$, the agents both prefer their own endowment to the other’s. When the profile is $(\theta'_i, \theta_j, \theta_{-i,-j})$, or $(\theta_i, \theta'_j, \theta_{-i,-j})$, they both prefer $i$’s endowment.

| A   | B   | A   | B   | A   | B   | A   | B   |
|-----|-----|-----|-----|-----|-----|-----|-----|
| x or $x'$ | x   | x   | x   | x   | x'  | x'  | x'  |
| B   | x'  | x   | x'  | x   | x   |  x' | x   |
|     |     |     |     |     |     |     |     |

**TABLE II**

OUTCOMES FOR EXAMPLE IN FIGURE 1 UNDER AN ARBITRARY EFFICIENT CHOICE RULE (LEFT); UNDER AN EFFICIENT CHOICE RULE WHICH BREAKS TIES LEXICOGRAPHICALLY ($\phi^{\text{SKM}}$) (MID-LEFT, MIDDLE); UNDER A SERIAL DICTATORSHIP $\phi^{\text{sd}}$ (MID-RIGHT, RIGHT)
and j’s endowment, respectively. When \((\theta'_i, \theta'_j, \theta_{-i,-j})\), they each prefer the other’s endowment to their own. Let \(x\) be the outcome in which both agents retain their endowment, i.e. \(x = (i, e(i)), (j, e(j))\). Let \(y\) be the outcome in which each agent gets each other’s endowment \(y = (i, e(j)), (j, e(i))\). Then, individual rationality makes the requirements shown on the mid-left in Figure 4: \(\phi(\theta_i, \theta_j, \theta_{-i,-j}) = (\theta_i, \theta'_j, \theta_{-i,-j}) = (\theta'_i, \theta_j, \theta_{-i,-j}) = x\). Meanwhile, efficiency requires \(\phi(\theta_i, \theta_j, \theta_{-i,-j}) = y\) (shown on the mid-right in Figure 4). Hence, by the Corners Lemma, no individually rational and efficient choice rule is contextually private under sequential elicitation protocols.

Q.E.D.

Also in two-sided matching, contextual privacy is incompatible with stability (also known as no justified envy) under sequential elicitation. In two-sided matching, every agent is matched to at most one object, and at most \(\kappa(c)\) agents are matched to school \(c\), for every \(c \in \mathcal{C}\), for some capacities \(\kappa(c)\). That is, the set of outcomes is

\[
\mathcal{X} = \{\mu \subseteq \mathcal{N} \times \mathcal{C}: \forall i \in \mathcal{N}: |\{c \in \mathcal{C} | (i, c) \in \mu\}| \leq 1 \text{ and } \forall c \in \mathcal{C} |\{i \in \mathcal{N} : (i, c) \in \mu\}| \leq \kappa(c)\}
\]

We say there is no oversupply if the aggregate capacity equals the number of agents, \(\sum_{c \in \mathcal{C}} \kappa(c) = n\).

We assume that objects have preferences over agents, which are given by priority scores. We assume the scores for different objects are private information of the agents. This matches the college assignment problem with standardized test scores (Balinski and Sönmez, 1999, Sönmez and Ünver, 2010). We assume that each agent (student) has a vector of scores \(s_c\), representing their score at each object (school) \(c \in \mathcal{C}\). Objects prefer agents with higher scores. Agent \(i\) has private information \(\theta_i = (\prec_i, s_i)\), where \(\prec_i\) is \(i\)’s preference ranking over schools, and \(s_i: \mathcal{C} \rightarrow \mathbb{R}\) maps objects to scores.

In such school choice settings, a desirable property of choice rules is stability. A choice rule \(\phi\) is stable or induces no justified envy if there is no pair \((i, c), i \in \mathcal{N}, c \in \mathcal{C}\) such that \(c \succ_i \phi_i(\theta)\) and \(s_i(c) > s_i(\phi_i(\theta))\).

**Theorem 1:** Assume there are \(n \geq 2\) agents, \(|\mathcal{C}| \geq 2\) objects and no oversupply. Then there is no stable and contextually private choice rule under sequential elicitation.

This finding is interesting in light of stability’s incompatibility with property of choice rules defined for extensive-form mechanisms: Ashlagi and Gonczarowski (2018) shows that stability is also not compatible with obvious strategy-proofness (Li, 2017).
3.2. Limits of Contextual Privacy in Auction Domains

We next consider single-item auctions and double auctions. Our results that pertain to the first-price and second-price auctions parallel prior results in a literature on decentralized computation, Brandt and Sandholm (2008).

Consider a standard private values auction environment in which a single indivisible item is to be allocated to one agent. Agents \( i \in N \) with types \( \theta_i \in \Theta \subseteq [0, 1] \), \( |\Theta| < \infty \). The outcomes are given by \( (q_i, t_i) \), \( q_i \in \{0, 1\} \), \( t_i \in \mathbb{R} \), where \( q_i \) is agent \( i \)'s allocation, and \( t_i \) is their payment. Preferences are defined by

\[
u_i((q, t), \theta_i) = 1_{q_i = 1} v_i(\theta_i) - t_i, \tag{5}
\]

where \( v_i : \Theta \to \mathbb{R} \). We call an auction standard if there is at most one agent \( i \in N \) such that \( t_i \neq 0 \) and \( q_i = 1 \). We call an auction efficient if

\[
\phi(\theta) \in \arg\max_{(q(\theta), t(\theta))} \sum_{i \in N} u_i((q(\theta), t(\theta)), \theta_i)
\]

for all \( \theta \in \Theta \).

The two most widely studied standard auction rules are the first-price and the second-price auction. As this article considers deterministic mechanisms, we consider these rules with deterministic tie-breaking which we without loss assume to be lexicographic. The first-price auction is a choice rule \( \phi_{FP}(\theta) = ((\phi_{FP}^1(\theta), ..., \phi_{FP}^n(\theta))) = ((q_1, t_1), ..., (q_n, t_n))(\theta) \), where

\[
\phi_{FP}^i(\theta) = \begin{cases} (1, \theta_i) & \text{if } \theta_i = \min \arg\max_{j \in N} \theta_j \\ (0, 0) & \text{otherwise.} \end{cases}
\]

The second-price auction is a choice rule \( \phi_{SP}(\theta) \), where

\[
\phi_{SP}^i(\theta) = \begin{cases} (1, \theta_{[2]}) & \text{if } i = \min \arg\max_{j \in N} \theta_j \\ (0, 0) & \text{otherwise.} \end{cases}
\]

Both of these auction rules can be implemented via a number of different protocols. Commonly studied protocols for the first-price and second-price rules, respectively, include the descending (“Dutch”) protocol and the ascending (“English”) protocol.

The second-price auction and its implementation as an ascending protocol is celebrated because it is not only efficient but also strategyproof (Vickrey, 1961, Wilson, 1989) and credible (Akbarpour and Li, 2020). Paralleling the result (Brandt and Sandholm, 2005, Theorem 4.9) for decentralized protocols, we show that the ascending auction protocol is not contextually private, and furthermore, that the second-price choice rule does not have a contextually private implementation.

**Proposition 4:** Assume \( n \geq 3 \) agents and \( |\theta| \geq 3 \). Under sequential elicitation, the second-price choice rule \( \phi^{SP} \) is not contextually private. If \( n \geq k + 2 \), the uniform \( k \)-th price auction is not contextually private.

**Proof:** The proof uses the Corners Lemma. Consider a type profile with \( \theta_{[1]} > \theta_{[4]} \) (or no constraint if \( n = 3 \)), and consider agents \( i, j \) that have types in \( \bar{\theta}, \hat{\theta} \) such that \( \theta_{[4]} < \bar{\theta} < \hat{\theta} < \theta_{[1]} \). Consider the product set \( \{\theta, \hat{\theta}\} \times \{\bar{\theta}, \hat{\theta}\} \times \times_{k \in N \setminus \{i, j\}} \theta_k \). This corresponds to a square depicted in Figure 5.
Let \( x \) be the outcome in which the highest type wins (\( q_i = 1 \) for \( \theta_i = \theta_{i,1} \), \( q_i = 0 \) otherwise) and pays the price \( t_i = \theta \). Let \( x' \) be the outcome under which the highest type wins and pays the price \( t_i = \bar{\theta} \). Then, \( \phi^{SP}(\theta, \bar{\theta}, \theta_{-i,-j}) = \phi^{SP}(\bar{\theta}, \bar{\theta}, \theta_{-i,-j}) = \phi^{SP}(\theta, \bar{\theta}, \theta_{-i,-j}) = x \). But, under \( \phi^{SP} \), it must be the case that \( \phi(\bar{\theta}, \bar{\theta}, \theta_{-i,-j}) = x' \). Since \( x \neq x' \), the Corners Lemma is violated, and thus the second-price choice rule is not contextually private under sequential elicitation.

An analogous construction is possible for the \( k \)-th price auction by considering agents \( i, j \) with types \( \bar{\theta}, \bar{\theta} \in (\theta_{[k-1]}, \theta_{[k+2]}) \).

Q.E.D.

We show in Appendix C that this impossibility holds even if ties are ruled out.

While second-price auctions are incompatible with contextual privacy, there are contextually private implementations of the first-price auction. Such an implementation is given by a descending protocol. A descending protocol queries, for each element of the type space \( \Theta \), this leads to a set of nodes \( N \times \Theta \times \{0, 1\} \) and edges from \( ((i, \theta, 0) \rightarrow (i + 1, \theta, 0)) \), for \( i \in N \setminus \{n\} \) and \( \theta \in \Theta \). There are edges from \( (n, \theta, 0) \) to \( (1, \max_{\theta' < \theta} \theta', 0) \). Furthermore, there are edges \( ((i, \theta, 0), (i, \theta, 1)) \) for all \( i \in N \) and \( \theta \in \Theta \) corresponding to an agent stating that they have a type \( \theta \), which leads to them being allocated the good. Hence, the set of terminal nodes is \( \Theta \times N \times \{1\} \). The associated set of type profiles is recursively defined as

\[
\Theta_{(i+1,\theta,0),i} := \Theta_{(i,\theta,0),i} \setminus \{\theta\}, \quad \Theta_{(i,\theta,1),i} := \{\theta\}, \quad \Theta_{(1,\theta,0),i} := \Theta_{(n,\max_{\theta' < \theta} \theta',0),i} \setminus \{\theta\}.
\]

The first rules out the type \( \theta \) for type \( i \) when they claim that they are not type \( \theta \). The second identifies an agent’s type exactly when they claim they are type \( \theta \). The last rules out the type \( \theta \) for agent \( n \) when they claim they are not \( \theta \) and leads to the protocol considering the next-lowest type \( \max_{\theta' < \theta} \theta' \).

**PROPOSITION 5:** The descending protocol for the first-price rule \( \phi^{FP} \) is contextually private under sequential elicitation.

Hence, the first-price choice rule is contextually private under sequential elicitation. The next example gives insight into the other kinds of standard auction choice rules that have contextually private implementations under sequential elicitation protocols.

**EXAMPLE:** Consider a standard auction rule in which the agent with the highest type wins and pays a price \( t \) where \( t: \Theta \rightarrow \mathbb{R} \) is an injective function. That is, the payment \( t \) that the winner pays is different for every type profile \( \theta \in \Theta \). In this case, the outcome \( \phi(\theta) = (q(\theta), t(\theta)) \) is different for every type profile. Hence, contextual privacy is trivial, as \( \phi(\theta) \neq \phi(\theta') \) for any \( \theta \neq \theta', \theta, \theta' \in \Theta \). Hence, any protocol that implements this auction rule is contextually private.
The example above shows that if the winner’s payment can depend in an arbitrary way on the profile of bids, many standard auction choice rules are contextually private. However, with an additional condition on how the payment depends on the bid distribution, the first-price choice rule is the unique contextually private choice rule. We say that payments in an auction depend only on rank if the payment is a function of an order statistic, \( t(\theta) = f(\theta_{[k]}), k \in \mathcal{N} \).

**Proposition 6:** Consider the class of choice rules \( \Phi \) that consists only of standard auctions where the payment \( t \) depends only on rank. Under sequential elicitation protocols, the first-price choice rule \( \phi^{FP} \) is the unique efficient and contextually private standard auction rule in \( \Phi \).

We conclude this section with a similar impossibility for standard double auction price rules. Suppose \( m \) agents are buyers and \( m \) agents are sellers, and \( n = 2m \). The \( m \) sellers are each endowed with one homogeneous, indivisible object. The buyers have unit demand for objects. Formally, agents have initial endowments \( e(i) \in \{0, 1\} \) where \( e(i) = 0 \) for buyers and \( e(i) = 1 \) for sellers. The preferences are

\[
u_i((q, t), \theta) = -e(i)v_i(\theta_i)q_i + (1 - e(i))v_i(\theta_i)q_i + t_i.
\]

A double auction price rule seeks to find a price \( t \) that maximizes \( \sum_{i \in \mathcal{N}} u_i((q, t), \theta_i) \) if buyers with types \( \theta_i \geq t \) buy a good at price \( t \), and sellers with value \( \theta_i \leq t \) sell their good at price \( t \). Agents with \( \theta_i = t \) sell or buy in order to match supply to demand.

**Proposition 7:** Assume there are \( n > 3 \) agents. There is no efficient, uniform-price contextually private double auction price rule under sequential elicitation protocols.

The main observation for this statement is that efficient price rules set prices that are medians of the empirical type distribution of types, \( \phi(\theta) \in [\theta_{[m]}, \theta_{[m+1]}] \). We prove that medians may not be computed in a contextually private way under sequential elicitation.

The next section shows how count queries allow for contextually private implementations for many mechanisms that may be formulated as matching supply and demand.

4. CONTEXTUAL PRIVACY AND TÂTONNEMENT

Thus far, we have studied contextual privacy in very restrictive environments. That is, we severely limited the set of tools that the designer could use to construct communication or access protocols. After all, part of our goal in defining contextual privacy—as outlined in Section 1—is to understand the demands of privacy in primitive technological environments. We required, in Section 3, that the designer access only one kind of query: the designer can only ask one agent at a time a yes-or-no question of the form “Does your type lie in subset \( \tilde{\theta} \) of \( \Theta \)?” In these restrictive environments, we found that contextual privacy is a demanding criterion—among common choice rules, Section 3 showed that only the serial dictatorship and the first-price auction have contextually private implementations.

In this section, we discuss mechanisms that preserve the spirit of contextual privacy, but require more advanced technology than allowed for in Section 3. To motivate our analysis, consider the following implementation of a second-price auction, which we showed to have no contextually private implementation in Section 3. Each agent has a willingness to pay \( \theta_i \in \Theta \). Agents submit bids in a set of \( |\Theta| - 1 \) sealed (tamper-evident) envelopes. Each envelope contains agent \( i \)’s answer to the question “Is your bid above \( \theta \)?” The envelopes are labelled
by $\theta$, the value asked about, and are submitted anonymously. The designer then runs a version of an ascending protocol with the anonymized envelopes, opening all of the envelopes with labels $\theta \in \Theta$ in increasing order. The designer stops opening envelopes at $\hat{\theta}$, when there is a single envelope that contains the answer “yes”. At this point, the designer can announce to all participants, “The price of the object is $\theta$, if you placed a bid above $\hat{\theta}$, please come forward to claim the object.” This final round does identify the winner, but it does so in a way that is reminiscent of a serial dictatorship under sequential elicitation protocols: the participant reveals herself only when she is directly changing the allocation.

With this implementation, the designer does not learn losing bidders’ exact values, it only learns that all losing bidders had values below $\hat{\theta}$. It also doesn’t learn the exact value of the winner, it only learns that the winner’s value is above $\hat{\theta}$. Moreover, the designer can send back all the un-opened envelopes, so that participants can verify that the designer learned only what it needed. In an important sense, the designer only learns what it needed to know—and thus it seems that there is, in fact, a contextually private implementation of the second-price auction.

The root of the contradiction between the seemingly-contextually private protocol just described and the impossibility result in Section 3 lies in the technology available to the designer. In the protocol described, we assumed that there is some trusted method through which the participants could de-identify their bids.

While such technologies may not be available or trusted in some settings, in other settings, there may be simple, inexpensive, and easy-to-explain technologies that offer sufficient (contextual) privacy to participants. Consider again Google’s ad auctions, discussed at the beginning of this paper. In a way that we will formalize in this section, Google’s second-price auctions could be made contextually private with a trusted technology that allowed advertisers to bid anonymously, and reveal their identities only when they win the auction. That is, there would have to be a digital version of the de-identified tamper-evident envelopes. Such an implementation would prevent Google from using identified advertisers’ history of losing bids to set personalized reserve prices. It would also be simpler and less costly to implement than sophisticated cryptographic techniques, which can be expensive in terms of computational power, implementation costs and auditing costs.

4.1. Tâtonnement Protocols are Contextually Private

To begin to understand the sense in which the implementation of the second-price auction described above is contextually private, we note that many mechanisms in the real world have a phased structure. That is, there are distinct phases that have distinct informational demands, and the outcome of one phase determines the set of possible outcomes for the next phase. For instance, in the “price mechanism,” prices are determined and then agents buy and sell products. The price that is determined changes the set of agents that buy and sell products. In school choice, a supply-demand approach establishes score cutoffs for each school, which are used in conjunction with student preferences to determine allocations (Azevedo and Leshno, 2016, Leshno and Lo, 2021).

We formally define a phase of a protocol as follows. Denote the precedence order in a protocol by $\prec$, i.e. $v \prec w$ says that node $v$ comes before node $w$.

**Definition:** Let $P = (V, E)$ be a protocol. We say that $V' \subseteq V$ is a phase of the protocol if for all $u, w \in V'$, if $u \prec v \prec w$, then $v \in V'$. We call a phase initial if it contains the root of $P$.

---

9The fact that the ascending protocol protects the winner’s privacy is noted in Milgrom and Segal (2020) and Ausubel (2004).
This definition suggests that there is no path through the protocol that leads out of a phase and back into it again.

We are interested in a particular class of two-phase protocols, which we will call tâtonnement protocols. We call these protocols tâtonnement protocols because there is a phase akin to price-finding, followed by a phase that determines allocation, thus mirroring the descriptions of price-finding and price-taking in Walras (1874).

To formally define tâtonnement protocols, we introduce the following notation. We denote the set of outcomes that a query $v$ leads to by $X_v := \phi(\Theta_v)$. We define $\text{end}(V')$ to be the latest elements in phase $V'$ under precedence order $\prec$. We denote subtree of the protocol following node $v'$ by $P_{v'}$.

**Definition:** A protocol $P = (V, E)$ for choice rule $\phi$ with initial phase $V'$ is a tâtonnement protocol if: (i) for each $v, w \in \text{end}(V')$ the set of outcomes following node $v$, $X_v$, and the set of outcomes following node $w$, $X_w$, are disjoint (i.e. $X_v \cap X_w = \emptyset$), and (i) the subtree of the protocol following node $v$, $P_{v'}$, is contextually private for $\phi$.

The key idea in this definition is that at the end of the first phase, the designer has information that leads to disjoint outcomes. For instance, the implementation of the second-price auction rule defined at the beginning of this section is a tâtonnement. The first phase is the phase conducted with the anonymized envelopes—the “price-finding” phase. The second phase is the one in which the highest bidder reveals herself and buys the object. Note that different conclusions to the price-finding phase lead to different outcomes in the “price-taking” phase, and the price-taking phase is akin to a serial dictatorship (and is thus contextually private). If the price turns out to be $\hat{\theta}$, then the bidder with a value above $\hat{\theta}$ gets the object and pays $\hat{\theta}$. If the price had turned out to be $\hat{\theta}'$, the bidder with value above $\hat{\theta}'$ gets the object and pays $\hat{\theta}'$. This is the sense in which the conclusion of the price-finding phase generates disjoint outcomes in the price-taking phase.

The following result contains the key insight of this section.

**Theorem 2:** Tâtonnement protocols are contextually private.

**Proof:** Let $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ be in different terminal nodes of $P$ with earliest point of departure $v$. There are two cases.

First, consider $v \in V'$ or $v \prec v'$ for $v' \in V$. Note that then the outcome associated to $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ are different as $X_{v'}, v' \in V'$ are disjoint.

Otherwise, $v \in V(P_{v'})$ for some $v' \in V'$. By contextual privacy of $P_{v'}$, $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ lead to different outcomes.

Q.E.D.

Theorem 2 is quite general. Note that it does not place any restrictions on the set of available protocols: it simply says that if there exists a contextually private implementation of the second phase, and the first phase leads to disjoint outcomes, then the implementation is contextually private. To interpret this result in a way that can guide design, we investigate the simplest implementations of tâtonnement protocols.

### 4.2. Many Auctions Can Be Implemented with a Simple Tâtonnement Protocol

Without discussing the restrictions on the designer’s technological environment, it is clear to see that many auctions have tâtonnement implementations and are thus contextually private. However, on its own, this result does not guide design: when arbitrarily sophisticated protocols
are available, almost any choice rule has a contextually private implementation. So, in this section, we ask which choice rules have a tâtonnement protocol that employs only individual elicitation queries (as studied in Section 3) and count queries (defined in Section 2). Recall that a count query asks about the number of agents whose type satisfies a particular property.

**Corollary 2:** The uniform \((k + 1)st\) price auction is contextually private with individual elicitation and count queries on type spaces \(\Theta = \{\theta \in \Theta : \theta_{[k + 1]} \neq \theta_{[k]}\}\). That is, the second-price auction is contextually private with count queries if first and second highest bid are not equal to each other.

**Corollary 3:** The Walrasian double auction is contextually private with count queries if \(\theta_{[n/2]} \neq \theta_{[n/2+1]}\).

To get a sense of why Corollary 2 and Corollary 3 hold, consider again the ascending implementation of the second-price auction described at the beginning of this section. This protocol is tâtonnement with only count queries and individual elicitation queries. In phase one of the protocol, all queries are count queries of a particular market clearing form: Is the number of agents that would be (strictly) willing to buy above a certain price exactly equal to the supply, which is a single good? Formally, these market-clearing queries are binary queries separating

\[
\{\theta \in \Theta : |\{i \in \mathcal{N} : \theta_i > \theta\}| = 1\}
\]

from

\[
\{\theta \in \Theta : |\{i \in \mathcal{N} : \theta_i > \theta\}| \neq 1\}
\]

for some potential price \(\theta\). The first time a query results in (6), a price is found, and agents \(i = 1, 2, \ldots, N\) are, sequentially, queried \(\{\theta \in \Theta : \theta_i > \theta\}\), i.e. “Is your type above \(\theta\)?” If agent \(i\)’s answer is “yes”, the protocol terminates and allocates the good to agent \(i\). Note that this protocol may never terminate if there is no single type such that (6) holds, which might be the case if the hypotheses of Corollary 2 (and, correspondingly, Corollary 3) did not hold.

### 4.3. Tâtonnement Requires Complex Queries in Matching Domains

A recent literature in market design has illustrated how many matching mechanisms can be understood in a supply-demand framework. Azevedo and Leshno (2016) develop a supply-demand framework for two-sided matching, showing that priority scores play a role similar to prices in the process that leads to stable allocations. In a similar vein, Leshno and Lo (2021) characterize the top-trading cycles assignment mechanism in terms of cutoffs between pairs of schools. Again, these cutoffs play a role similar to prices in a competitive equilibrium framework.

The protocols that lead to stable allocations described by Azevedo and Leshno (2016) and the protocols that implement top-trading cycles described in Leshno and Lo (2021) both structurally resemble tâtonnement protocols. There is an initial phase that partitions the protocol tree into sub-trees that lead to disjoint sets of outcomes, and there is a second phase that resembles a contextually private mechanism, serial dictatorship, in determining the final allocation.

However, condition (i) in the definition of tâtonnement is unlikely to hold when the designer can use only count queries. An algorithm where overdemanded schools increase admission cutoffs until no school is overdemanded provably converges to cutoffs that induce stability (Azevedo and Leshno, 2016, Proposition A2). While such a score-finding algorithm may be implemented using count queries that check the demand for a school, different nodes at the end
of such a phase may still lead to the same outcome: different queries at the end of a phase may correspond to the same score profile. This puts a limitation on implementations of contextual privacy in assignment domains, which we state and prove in Appendix A.

With more complex queries, some of these limitations can be overcome. Assume now that a query may simultaneously depend on the counts of \( l \geq 1 \) subsets of the type space \( \Theta \). With such multi-count queries, tâtonnement protocols for finding a stable allocation exists. After asking for every score profile \( \sigma \) “Is score profile \( s \) market-clearing?”, i.e. whether there is no over-demanded school at the given cutoffs. If the answer is yes, agents sequentially choose the most preferred school they are admitted to. If the scores are part of the outcome space, we show in Appendix A that there is a contextually private protocol with multi-count queries that produces a stable outcome for the school assignment problem.

5. EXTENSIONS

In this section, we consider two concepts that strengthen contextual privacy. We explore these stronger concepts for both theoretical and practical reasons. On the practical side, these extensions may have desirable properties in some settings. On the theoretical side, these criteria help to illuminate connections to other desiderata in mechanism design, and illustrate which of our results are robust to alternative formulations of contextual privacy. In this section, we revert to the assumption maintained throughout Section 3 that the designer has access only to sequential elicitation protocols.

5.1. Individual Contextual Privacy

The first extension, individual contextual privacy, requires that if two types are distinguishable for agent \( i \), these types must lead to different outcomes under \( \phi \) for agent \( i \). This definition thus only applies in domains where the outcome space \( X \), specifies an allocation for each agent \( i \in \mathcal{N} \). Let \( \phi_i(\theta) \) denote the projection of the outcome vector \( \phi(\theta) \) onto the \( i \)th component.

DEFINITION—Individually Contextually Private Protocols: A protocol \( P = (V, E) \) for a social choice function \( \phi \) is individually contextually private if for all terminal nodes \( z, z' \in Z_P \) and all type profiles \( (\theta_i, \theta_{-i}) \in \Theta_z, (\theta'_i, \theta_{-i}) \in \Theta_{z'} \),

\[
\phi_i(\theta_i, \theta_{-i}) \neq \phi_i(\theta'_i, \theta_{-i}).
\]

Notice that individual contextual privacy is stronger than contextual privacy—any choice rule that is contextually private is also individually contextually private. If there were an agent \( i \) for whom contextual privacy were violated, then individually contextual privacy would automatically be violated.

As a normative criterion, individual contextual privacy requires that if the designer can distinguish between two types for agent \( i \), then it should be the case that agent \( i \)’s outcome is changed. This criterion captures a notion of legitimacy—agent \( i \) may view participation in the mechanism as involving an inherent tradeoff between information revelation and allocation. We can imagine a speech from agent \( i \) along the following lines: “The designer can learn that I have type \( \theta_i \) and not \( \theta'_i \) as long as the designer’s knowledge of this makes a difference to my allocation.”

\[10\] The domains that we focus on in this paper—auction domains and assignment domains—both satisfy this property. Any domain with transfers also satisfies this property. However, voting rules, for example, do not have this property—there is a single social outcome, without individualized allocations.
Individual contextual privacy is closely related to non-bossiness, introduced by Satterthwaite and Sonnenschein (1981). A choice rule $\phi$ is non-bossy if for all $\theta_i \in \Theta$,

$$\phi_i(\theta_i, \theta_{-i}) = \phi_i(\theta'_i, \theta_{-i}) \implies \phi_i(\theta_i, \theta_{-i}) = \phi_i(\theta'_i, \theta_{-i})$$.

Non-bossiness says that if agent $i$ changes her report from $\theta_i$ to $\theta'_i$ and her allocation is unchanged, then no other agent $j$’s allocation changes either. The idea is that if agent $i$ could unilaterally change her report and affect a change in some agent $j$’s allocation without changing her own allocation, agent $i$ would be “bossy.” We show that non-bossiness is a necessary condition for individual contextual privacy, and individual contextual privacy lies at the intersection of contextual privacy and non-bossiness.

**Proposition 8:** A choice rule $\phi : \Theta \rightarrow X^n$ is individually contextually private if and only if it is contextually private and non-bossy.

**Proof:** Suppose for contradiction that protocol $P$ individually contextually privately implements $\phi$, but $\phi$ is bossy. Since $\phi$ is bossy, there exists a $j \in N \setminus \{i\}$ and type profiles $(\theta_i, \theta_{-i}), (\theta'_i, \theta_{-i})$ such that $\phi_i(\theta_i, \theta_{-i}) = \phi_i(\theta'_i, \theta_{-i})$ but $\phi_j(\theta_i, \theta_{-i}) \neq \phi_j(\theta'_i, \theta_{-i})$. Since $\phi_j(\theta_i, \theta_{-i}) \neq \phi_j(\theta'_i, \theta_{-i})$, any protocol $P$ that implements $\phi$, including $P$, must have $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ in distinct terminal nodes $z, z'$ (otherwise $P$ could not certify $\phi$). But if $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ belong to distinct terminal nodes in $P$ and $P$ contextually privately implements $\phi$, it must be that $\phi_i(\theta_i, \theta_{-i}) \neq \phi_i(\theta'_i, \theta_{-i})$, which contradicts the assumption that $\phi$ is bossy.

Next, assume that $\phi$ is non-bossy and contextually private. Consider $(\theta_i, \theta_{-i})$ and $(\theta'_i, \theta_{-i})$ in distinct terminal nodes of protocol $P$. By contextual privacy, $\phi(\theta_i, \theta_{-i}) \neq \phi(\theta'_i, \theta_{-i})$. By non-bossiness, $\phi_i(\theta_i, \theta_{-i}) \neq \phi_i(\theta'_i, \theta_{-i})$ follows. Thus, $P$ is contextually private. Q.E.D.

This characterization results in unique characterizations for the first-price auction and the serial dictatorship.

**Proposition 9:** Serial dictatorships are the unique individually contextually private, efficient and strategyproof object assignment rules.

**Proof:** The serial dictatorship contextually private and non-bossy, hence individually contextually private by Proposition 8. It also is strategyproof.

Conversely, if $\phi$ is individually contextually private, then it is also non-bossy by Proposition 8. It is known that the only efficient, strategyproof and non-bossy object assignment mechanisms are serial dictatorships (see Hatfield (2009) for a proof, and compare Satterthwaite and Sonnenschein (1981)). Q.E.D.

**Proposition 10:** The first-price auction is the unique individually contextually private, efficient, and individually rational auction rule.

**Proof:** The first-price auction is individually contextually private. Indeed, the protocol outlined in Section 3 is individually contextually private. It is well known that the first-price auction is efficient and individually rational.

Let $\phi$ be any individually contextually private, efficient and individually rational auction rule. By Pycia and Raghavan (2022, Theorem 1), this means that it implements (up to a zero set) a first-price auction. Q.E.D.

---

11 See Thompson (2014) for a discussion of the normative content of non-bossiness.
5.2. Group Contextual Privacy

Another extension is group contextual privacy. Group contextual privacy requires that if two type profiles are distinguishable at the end of the protocol, then they must lead to different outcomes. This notion strengthens contextual privacy, which requires only that if a single agent’s types are distinguishable, then they lead to different outcomes.

**Definition—Group-Contextual Privacy:** A protocol $P = (V, E)$ for a social choice function $\phi$ is contextually private if for all terminal nodes $z, z' \in Z_P$ and all type profiles $\theta \in \Theta_z, \theta' \in \Theta_{z'}$, $\phi(\theta) \neq \phi(\theta')$.

Notice again that this definition strengthens contextual privacy. Here, it is because it strengthens the underlying notion of distinguishability—two type profiles $\theta, \theta'$ are distinguishable if they belong to different terminal nodes. Regular contextual privacy’s notion of distinguishability is on the agent-level—two types $\theta_i, \theta'_i$ are distinguishable if they belong to different terminal nodes, holding all other agent’s types fixed at $\Theta_{-i}$.

We characterize the set of group contextually private protocols next. First, recall from Section 4 that we denote the set of outcomes reachable from node $v$, labelled with $\Theta_v$ by $X_v := \phi(\Theta_v)$.

**Theorem 3:** A protocol $P = (V, E)$ is group contextually private under a class of protocols $\mathcal{P}$ if and only if for any query, $\bigcup_{(v, w) \in E} X_w = X_v$ is a disjoint union.

**Proof:** First assume that $P$ is group contextually private, and assume for contradiction that $v$ is a query such that $(v, w), (v, w') \in E$ and $X_w \cap X_{w'} \neq \emptyset$. Hence, there are $\theta \in \Theta_w$ and $\theta' \in \Theta_{w'}$ such that $\phi(w) = \phi(w')$, which contradicts group contextual privacy.

Next assume that reachable outcomes are disjoint at each query. Let $\theta$ and $\theta'$ have earliest node of departure $v$. As outcomes are disjoint, it must be that $\phi(\theta) \neq \phi(\theta')$. Hence the protocol is group contextually private.

Q.E.D.

This general characterization lends more practical insight when specialized to group contextual privacy under only sequential elicitation protocols.

**Corollary 4:** A social choice function is group contextually private under sequential elicitation protocols if and only if it can be represented by a protocol in which, at every node, the agent’s choice rules out a subset of the outcomes.

This characterization, in particular, implies that the serial dictatorship is group contextually private. In a live sequential implementation of a serial dictatorship, whenever an agent is called to play, they obtain their favorite object among those that remain. So, their choice rules out the outcomes in which a different agent gets their favorite object that remains.

Group contextual privacy, under sequential elicitation protocols, is thus reminiscent of other extensive-form properties related to simplicity that the serial dictatorship satisfies. In particular, the serial dictatorship is obviously strategyproof Li (2017) and strongly obviously strategyproof Pycia and Troyan (2021).

Is there a containment relationship between protocols that are group contextually private and obviously strategyproof? It turns out that the answer is no: there are mechanisms that are group contextually private and not obviously strategyproof, and vice versa. The ascending auction is obviously strategyproof Li (2017), but not group contextually private with respect to
sequential elicitation, as it implements the second-price auction, which is not contextually private, as seen in Section 3. A class of “non-clinching rules”, on the other hand, are strategyproof and group contextually private, but fail to have an obviously strategyproof implementation. Appendix B offers an example of a non-clinching rule, and shows that it is group contextually private but not obviously strategyproof.

6. RELATED LITERATURE

This paper brings privacy considerations into the tradition of extensive-form mechanism design.

An extensive-form criterion that is closely related to contextual privacy in motivation is credibility (Akbarpour and Li, 2020). Credibility requires incentive compatibility for the auctioneer, and offers a different diagnosis of the issues with the second-price auctions used by Google and discussed in Section 1. While contextual privacy tells us that the second-price auction is not private, and thus needs to be implemented with a privacy-preserving protocol, credibility would say that the problem is that the second-price auction is not credible—the auctioneer has an incentive to deviate from their stated plan. Though the two diagnoses coincide in the case of the second-price auction (as the second-price auction is neither contextually private nor credible), and the first-price auction (as the first-price auction is both contextually private and credible) further connections are hard to established as incentives of the designer are ambiguous in other domains. Credibility requires an unambiguous formulation of the designer’s incentives—assignment domains are difficult to analyze through the lens of credibility, because the designer’s incentives are not straightforward. Contextual privacy, on the other hand, extends readily to these domains, as it does not depend on the designer’s incentives.

As noted throughout the text, contextual privacy (with sequential elicitation) parallels the concept of unconditional full privacy for decentralized protocols (Brandt and Sandholm, 2005, 2008). Unconditional full privacy requires that the only information revealed through a decentralized protocol is the information contained in the outcome. In its standard formulation, it is not amenable to a mechanism design framework in which a principal chooses an allocation based on participants’ information. Unconditional full privacy has been applied to an auction domain (Brandt and Sandholm, 2008), and a voting domain (Brandt and Sandholm, 2005). In those works, the authors emphasize impossibilities and computational complexity of unconditional full privacy. For example, they present several results on the number of communication rounds needed in a protocol. We present a definition for contextual privacy in a formal framework amenable to economic analysis and mechanism design, and extend it in several ways: we discuss assignment domains, we add count queries, and we discuss extensions to group and individual contextual privacy. In addition, we strengthen the impossibility result Brandt and Sandholm (2008, Theorem 4.9) paralleling our Proposition 4 to cases where no ties are allowed (see the proof in Appendix C).

Milgrom and Segal (2020)’s concept of unconditional winner privacy is similar to contextual privacy in that it brings unconditional full privacy into centralized mechanism design: unconditional winner privacy is unconditional full privacy in a centralized mechanism, for the winner only. Contextual privacy differs from unconditional winner privacy in three ways: (i) we require privacy for all players while Milgrom and Segal require privacy for just the winner, (ii)

---

12 Another extensive form criterion that helped to emphasize the importance of dynamic implementation is obvious strategyproofness Li (2017), which has been widely studied, often in conjunction with other normative properties of mechanisms (Bade and Gonczarowski, 2016, Ashlagi and Gonczarowski, 2018, Mackenzie, 2020, Pycia and Troyan, 2021, Golowich and Li, 2021, Mackenzie, 2020, Mackenzie and Zhou, 2022).
we define the set of outcomes to be allocations and prices (whereas Milgrom and Segal define outcomes to be allocations alone), (iii) we define contextual privacy in a range of domains while Milgrom and Segal consider only the auction domain. So, while the ascending auction satisfies unconditional winner privacy because it protects the full willingness to pay of the highest bidder, we find that the ascending auction fails contextual privacy precisely because it does not protect the full willingness to pay of losing bidders.

Beyond unconditional full privacy, the most closely related concept in computer science and cryptography, lies an extensive literature on privacy preserving protocols for auctions and allocation. The literature on cryptographic protocols for auctions, going back to Nurmi and Salomaa (1993) and Franklin and Reiter (1996) is too vast to summarize here—the main point is that there are many cryptographic protocols that do not reveal any private information to a designer. Such protocols allow participants to jointly compute the outcome without relying on any trusted third party. To this literature we bring analysis of the impact of the social and technological environments in which many designers operate: when arbitrary cryptographic protocols are not available, we need some other privacy desideratum to guide design. Thus, we align with the tradition of contextual integrity Nissenbaum (2004) which contrasts with traditions that view cryptography as a go-to solution for all privacy problems (Benthall et al., 2017).

An influential privacy desideratum that also does not rely on cryptographic techniques is differential privacy (Dwork et al., 2006). Contextual privacy sharply diverges from interpretations of differential privacy in mechanism design contexts. Differential privacy, as adapted for mechanism design contexts, says that the report of a single agent should have a negligible effect on the outcome. (This idea also has a precedent in the concept of “informational smallness” studied in Gul and Postlewaite (1992) and McLean and Postlewaite (2002).) To illustrate the sharp contrast between differential privacy and contextual privacy, suppose some bit of information is revealed through the mechanism. Differential privacy says that this bit can be revealed if it does not have an effect (or has a negligible effect) on the outcome. Contextual privacy says that this bit can be revealed if it does have an effect on the outcome—it can be revealed if the designer needed to know it. Whether contextual or differential privacy is a more appropriate notion of privacy will depend on context.

Several authors have taken a non-axiomatic approach, incorporating measures of “privacy loss” as constraints on mechanism design. For instance, Eilat et al. (2021) define privacy loss to be the Kullback-Leibler divergence between the designer’s prior and her posterior. They study optimal mechanisms subject to a constraint on the privacy loss. In a similar vein, Liu and Bagh (2020) defines an information revelation measure using Shannon’s entropy. These measure-based criteria treat all datum as equal. Contextual privacy, unlike these measure-based criteria, is not about how much information is revealed, and is also not just about whether information is revealed, but rather it is about how the information that is revealed is used.

7. DISCUSSION

Contextual privacy can guide design when participants have concerns about the use of their private information, and when highly sophisticated cryptographic solutions are not available or are excessively costly. We find that few choice rules have contextually private implementations when the designer can only carry out protocols that resemble extensive-form games: among common choice rules, serial dictatorships and first-price auctions are exceptions. When

---

13Differential privacy was originally proposed as a tool for database management. For a survey of its incorporation into mechanism design, see Pai and Roth (2013).
designers can use count queries, many common auction rules have contextually private implementations, which take the form of tâtonnement protocols.

The results about tâtonnement protocols connect contextual privacy to foundational ideas about information and decentralization in economics. Hayek (1945) commented on how prices aggregate dispersed information in a decentralized way—that is, without needing to elicit and process individuals’ private information on a continuous basis. Even when studying centralized mechanisms, Hurwicz (1973) remarked “it is natural to seek computing procedures that would minimize the need for information transfers.” When these authors were writing, the desire to minimize information processing came about because of limitations on computing power. Now, centralized platforms continually process an abundance of data in order to elicit preferences and precisely tune outcomes on a continual basis. Some have remarked that such platforms make our predecessors’ fears about about the scale of information processing needed in a centralized system appear quaint (Morozov, 2019). Even if the computational burdens of centralized information processing have lifted since Hayek and Hurwicz, contextual privacy highlights another good reason to search for information-minimal implementations of market rules. Indeed our result that tâtonnement protocols are contextually private suggests that privacy is another virtue of decentralized price systems, and that certain forms of privacy can be preserved in centralized implementations with simple technologies.

Contextually private implementation raises a number of avenues for further research. In particular, this paper did not discuss randomized protocols or choice rules, which would dramatically change the set of contextually private choice rules—though also may occasion a modified definition of contextually privacy to preserve its spirit in the face of randomness. Relatedly, we did not introduce statistical queries on protocols, which would allow, for example, an articulation of—and more direct comparison to—differential privacy (Dwork, 2006) within our framework. In addition, in further work we hope to explore relative and approximate notions of contextual privacy which would give insight into the degree to which different mechanisms satisfy or violate contextual privacy.

APPENDIX: Additional Proofs

Proof of Proposition 2: Consider \( \theta_i, \theta_i' \in \Theta \) and a partial type profile for other agents \( \theta_{-i} \in \Theta^{n-1} \) such that \((\theta_i, \theta_{-i})\) is separated from \((\theta_i', \theta_{-i})\). We will show that \( \phi(\theta_i, \theta_{-i}) \neq \phi(\theta_i', \theta_{-i}) \).

Denote \( A \) the node of separation. By definition of sequential elicitation, this must be a query to agent \( i \). By definition of serial dictatorship, the children of \( A \) are given by \( \{\theta|\theta_{π(i)} \in \max_{θ_{π(i)}} R(i) = c\} \) for some \( c \in R(A) \). Hence, if \( \phi(\theta_i, \theta_{-i}) \) and \( \phi(\theta_i', \theta_{-i}) \) are separated from each other, agent \( i \) must get a different assignment under \( \theta_i \) and \( \theta_i' \), hence \( \phi(\theta_i, \theta_{-i}) \neq \phi(\theta_i', \theta_{-i}) \). Q.E.D.

Proof of Theorem 1: The proof uses the Corners Lemma. We first choose the type profile for \( n-2 \) agents that are not labelled \( i \) or \( j \). Then we construct a square representing possible types for agents \( i \) and \( j \).

Let \( s_1 > s_2 > s_3 > s_4 \). Fix the type profile of all \( n-2 \) agents that are not \( i \) or \( j \) to be \( \theta_{-i,-j} \) where each agent has a score greater than \( s_1 \) for their top choice object, and their top choice object has capacity to accommodate them. Denote \( C \) there is no oversupply, i.e. \( \sum_{c \in C} \kappa(c) = n \), the number of remaining spots is \( n - (n-2) = 2 \). Assume without loss of generality that the remaining spots are for different objects. Label these objects with remaining spots \( a \) and \( b \).

Consider the final two agents \( i, j \in N \). Two possible (partial) types for agent \( i, j \) are:

\[ \theta_i = (a \succ_i b, s_i(a) = s_1, s_j(b) = s_4), \quad \theta_i' = (b \succ_i a, s_i(a) = s_3, s_j(b) = s_2) \]
belong to the set
For ease of exposition (and without loss of generality), suppose these middle four types are
and considers all possible combinations in
choice rule, it suffices to show that no Walrasian choice rule is contextually private.

Let, without loss, \( \theta_i, \theta_i' \) and \( \theta_j, \theta_j' \) be separated. By definition of sequential elicitation, this must happen when agent \( i \) is queried. Note that terminal nodes cannot separate type profiles. Hence, \( (\theta_i, \theta_{-i}) \) and \( (\theta_i', \theta_{-i}) \) are separated at a node of the form \((i, \tilde{\theta}, 0)\). By definition of the descending protocol, the children of the node \((i, \tilde{\theta}, 0)\) are associated to sets

\[
\{\tilde{\theta}\} \text{ and } \{\tilde{\theta}' \in \Theta : \tilde{\theta}' < \tilde{\theta}\}.
\]

Let, without loss, \( \theta_i = \tilde{\theta} \) and \( \theta_i' < \tilde{\theta} \). In the former case, the outcome is that agent \( i \) gets the good at price \( \tilde{\theta} \). By definition of the descending protocol, in the latter case, it is that either agent \( i \) does not get the good, or they get it at a price \( \tilde{\theta}' < \tilde{\theta} \).

Note that by construction of the protocol, the first query leading to a singleton possible type space must be a type \( \theta_i \) attaining \( \max_{i \in N} \theta_i \). This implies that the descending protocol implements a first-price choice rule (with tie-breaking according to the order \( 1, 2, \ldots, n \)). \( Q.E.D. \)

PROOF OF PROPOSITION 7. Since every efficient uniform-price choice rule is a Walrasian choice rule, it suffices to show that no Walrasian choice rule is contextually private.

We use the Corners Lemma. Consider four agents \( i, j, k, \) and \( \ell \) who have the types

\[
\{\theta_{[m-1]}, \theta_{[m]}, \theta_{[m+1]}, \theta_{[m+2]}\}.
\]

For ease of exposition (and without loss of generality), suppose these middle four types are belong to the set \( \{\tilde{\theta}, \tilde{\theta}\}^4 \) with \( \tilde{\theta} < \tilde{\theta} \). Consider arbitrary endowments.

We construct two squares: a square that holds agents \( k \) and \( \ell \)’s types fixed at \( (\theta_k, \theta_\ell) = (\tilde{\theta}, \tilde{\theta}) \) and considers all possible combinations in \( \{\tilde{\theta}, \tilde{\theta}\}^2 \) for agents \( i \) and \( j \); a square that holds \( i \) and \( j \)’s types fixed at \( (\theta_k, \theta_\ell) = (\tilde{\theta}, \tilde{\theta}) \) and varies \( k \) and \( \ell \) in the same manner. See Figure A.7.
Let $x$ be the outcome in which the market clearing price is $t = \theta$ and let $x'$ be the outcome in which the market clearing price is $t = \bar{\theta}$. Consider first the top square which holds the types of agents $k$ and $\ell$ fixed and varies the types of agents $i$ and $j$. Efficiency requires $\phi(\theta_i, \theta_j, \bar{\theta}, \bar{\theta}) = \phi(\theta_i', \theta_j', \bar{\theta}, \bar{\theta}) = \phi(\theta_i, \theta_j', \bar{\theta}, \bar{\theta}) = x$. Efficiency also requires that $\phi(\theta_i', \theta_j', \bar{\theta}, \bar{\theta}) \in \{x, x'\}$.

Now consider the bottom square which holds the types of agents $i$ and $j$ fixed and varies the types of agents $k$ and $\ell$. Efficiency requires $\phi(\bar{\theta}, \bar{\theta}, \theta_k, \theta_\ell) \in \{x, x'\}$. It also requires that $\phi(\bar{\theta}, \bar{\theta}, \theta_k', \theta_\ell) = \phi(\bar{\theta}, \bar{\theta}, \theta_k, \theta_\ell') = \phi(\bar{\theta}, \bar{\theta}, \theta_k', \theta_\ell') = x'$.

The outcome under the type profile in the box that conjoins the two squares $(\bar{\theta}, \bar{\theta}, \theta, \theta)$ must be either $x$ or $x'$ (it cannot be both). If it is $x$, then the Corners Lemma is violated in the bottom $(k - \ell)$ square. If it is $x'$, then the Corners Lemma is violated in the top $(i - j)$ square. So, there must be a violation of the Corners Lemma, and any efficient uniform-price rule is not contextually private under sequential elicitation protocols. 

**Proof of Proposition 6**: A similar construction as in the proof of Proposition 4. The quantile that the price depends on is chosen by two types. The Corners Lemma can be similarly applied.

**Proof of Corollary 2**: Consider the protocol that repeatedly queries

\[ \{\theta : |\{i \in \mathcal{N} : \theta_i > \theta\}| = k\} \tag{8} \]

versus

\[ \{\theta : |\{i \in \mathcal{N} : \theta_i > \theta\}| \neq k\} \]

for an increasing enumeration of $\Theta$. If (8) is reached, agents sequentially are queried $\{\theta \in \Theta : \theta_i > \theta\}$. Those for which this holds are allocated the item, others not. Allocated agents pay $\theta$. Note that the restriction on the type profiles $\{\theta \in \Theta : \theta_{[k+1]} \neq \theta_{[k]}\}$ yields that one of the queries (8) is reached and hence the goods are allocated. We claim that this is a tâtonnement protocol: the queries (8) form phase one (they lead to disjoint sets of outcomes) and the set of subtrees $P_v$ for each query $v$ is contextually private under sequential elicitation. For the former, note that the prices paid are different following different nodes (8). For the latter, note that any change of type that changes the outcome of a query would yield a different allocation. Therefore, the described protocol is a tâtonnement protocol which, by Theorem 2 means it is contextually private.

**Proof of Corollary 3**: We can specialize the protocol outlined in the proof of Corollary 2 with $k = \frac{n}{2}$, and a quaternary query asking $\{\theta \in \Theta : \theta_i > \theta\}$ and $e_i = 1$. Agents such that
\( \theta_i > \theta \) are allocated the object, and agents pay if they have not been endowed, but are allocated, resp. are paid if they are not allocated but have been endowed, \( \theta \).

\[ \text{Q.E.D.} \]

**BIBLIOGRAPHY**

AKBARPOUR, MOHAMMAD AND SHENGWU LI (2020): “Credible auctions: A trilemma,” *Econometrika*, 88, 425–467. [1, 5, 14, 23]

ALAWADHI, NEHA (2021): “Only 1 in 250 understand role of encryption in securing messaging: Study,” *Business Standard*, March 21. [2]

ALVAREZ, RAMIRO AND MEHRDAD NOJOUMIAN (2020): “Comprehensive survey on privacy-preserving protocols for sealed-bid auctions,” *Computers & Security*, 88, 101502. [2]

ASHLAGI, ITAI AND YANNAI A GONCZAROWSKI (2018): “Stable matching mechanisms are not obviously strategy-proof,” *Journal of Economic Theory*, 177, 405–425. [13, 23]

AUSUBEL, LAWRENCE M (2004): “An efficient ascending-bid auction for multiple objects,” *American Economic Review*, 94, 1452–1475. [17]

AZEVEDO, EDUARDO M AND JACOB D LESHNO (2016): “A supply and demand framework for two-sided matching markets,” *Journal of Political Economy*, 124, 1235–1268. [17, 19]

BADE, SOPHIE (2020): “Random serial dictatorship: the one and only,” *Mathematics of Operations Research*, 45, 353–368. [12]

BADE, SOPHIE AND YANNAI A GONCZAROWSKI (2016): “Gibbard-Satterthwaite success stories and obvious strategyproofness,” arXiv preprint arXiv:1610.04873. [23]

BALINSKI, MICHEL and TAYFUN SÖNMEZ (1999): “A tale of two mechanisms: student placement,” *Journal of Economic theory*, 84, 73–94. [13]

BENTHAL, SEBASTIAN, SEDA GÜRSES, HELEN NISSENBAUM, ET AL. (2017): *Contextual integrity through the lens of computer science*, Now Publishers. [24]

BOGETOFT, PETER, DAN LUND CHRISTENSEN, IVAN DAMGÅRD, MARTIN GEISLER, THOMAS JAKOBSEN, MIKKEL KROIGAARD, JANUS DAM NIELSEN, JESPER BUUS NIELSEN, KURT NIELSEN, JAKOB PAGTER, ET AL. (2009): “Secure multiparty computation goes live,” in *International Conference on Financial Cryptography and Data Security*, Springer, 325–343. [2]

BRANDT, FELIX and TUOMAS SANDHOLM (2005): “Unconditional privacy in social choice,” in *Theoretical Aspects of Rationality and Knowledge*, 207–218. [14, 23]

——— (2008): “On the existence of unconditionally privacy-preserving auction protocols,” *ACM Transactions on Information and System Security (TISSEC)*, 11, 1–21. [5, 14, 23, 32]

CAIN, ABBIGAIL (2018): “Before Envelopes, People Protected Messages With Letterlocking,” *Atlas Obscura*. [3]

CHOR, BENNY, MIHÁLY GÉRÉB-GRAÜS, and EYAL KUSHILEVITZ (1994): “On the structure of the privacy hierarchy,” *Journal of Cryptology*, 7, 53–60. [8]

CHOR, B. AND E. KUSHILEVITZ (1989): “A Zero-One Law for Boolean Privacy,” in *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, New York, NY, USA: Association for Computing Machinery, STOC ’89, 62–72. [8, 10]

DWORK, CYNTHIA (2006): “Differential privacy,” in *International Colloquium on Automata, Languages, and Programming*, Springer, 1–12. [5, 25]

DWORK, CYNTHIA, FRANK McSHERRY, KOBBI NISSIM, and ADAM SMITH (2006): “Calibrating noise to sensitivity in private data analysis,” in *Theory of cryptography conference*, Springer, 265–284. [24]

EILAT, RAN, KFIR ELIAZ, and XIAOSHENG MU (2021): “Bayesian privacy,” *Theoretical Economics*, 16, 1557–1603. [24]

FRANKLIN, MATTHEW K AND MICHAEL K REITER (1996): “The design and implementation of a secure auction service,” *IEEE Transactions on Software Engineering*, 22, 302–312. [24]

GOLOWICH, LOUIS AND SHENGWU LI (2021): “On the computational properties of obviously strategy-proof mechanisms,” arXiv preprint arXiv:2101.05149. [23]

GUL, FARUK AND ANDREW POSTLEWAITE (1992): “Asymptotic efficiency in large exchange economies with asymmetric information,” *Econometrika: Journal of the Econometric Society*, 1273–1292. [24]

HATFIELD, JOHN WILLIAM (2009): “Strategy-proof, efficient, and nonbossy quota allocations,” *Social Choice and Welfare*, 33, 505–515. [21]

HAYEK, FRIEDRICH AUGUST (1945): “The use of knowledge in society,” *The American economic review*, 35, 519–530. [25]

HURWICZ, LEONID (1973): “The design of mechanisms for resource allocation,” *The American Economic Review*, 63, 1–30. [25]
LESHNO, JACOB D AND IRENE LO (2021): “The cutoff structure of top trading cycles in school choice,” The Review of Economic Studies, 88, 1582–1623. [17, 19]
LI, SHENGWU (2017): “Obviously strategy-proof mechanisms,” American Economic Review, 107, 3257–87. [13, 22, 23]
LIU, DE AND ADIB BAGH (2020): “Preserving bidder privacy in assignment auctions: design and measurement,” Management Science, 66, 3162–3182. [24]
MACKENZIE, ANDREW (2020): “A revelation principle for obviously strategy-proof implementation,” Games and Economic Behavior, 124, 512–533. [23]
MACKENZIE, ANDREW AND YU ZHOU (2022): “Menu mechanisms,” Journal of Economic Theory, 204, 105511. [23]
MCLEAN, RICHARD AND ANDREW POSTLEWAITE (2002): “Informational size and incentive compatibility,” Econometrica, 70, 2421–2453. [24]
MILGROM, PAUL AND ILYA SEGAL (2020): “Clock auctions and radio spectrum reallocation,” Journal of Political Economy, 128, 1–31. [17, 23, 24]
MOROZOV, EVGENY (2019): “The Calculation Debate in the Age of Big Data,” NLR, 116. [25]
NISSENBAUM, HELEN (2004): “Privacy as contextual integrity,” Washington Law Review, 79, 119. [24]
NURMI, HANNU AND ARTO SALOMAA (1993): “Cryptographic protocols for Vickrey auctions,” Group Decision and Negotiation, 2, 363–373. [24]
PACHILAKIS, MICHALIS, PANAGIOTIS PAPADOPOULOS, EVANGELOS P MARKATOS, AND NICOLAS KOURTEL-LIS (2019): “No more chasing waterfalls: a measurement study of the header bidding ad-ecosystem,” in Proceedings of the Internet Measurement Conference, 280–293. [2]
PACIALIS, MICHALIS, PANAGIOTIS PAPADOPOULOS, EVANGELOS P MARKATOS, AND NICOLAS KOURTEL-LIS (2019): “No more chasing waterfalls: a measurement study of the header bidding ad-ecosystem,” in Proceedings of the Internet Measurement Conference, 280–293. [2]
PYCIA, MAREK AND MADHAV RAGHAVAN (2022): “Non-bossiness and First-Price Auctions,” Tech. rep., CEPR Discussion Paper No. DP16874. [4, 21]
PYCIA, MAREK AND PETER TROYAN (2021): “A theory of simplicity in games and mechanism design,” University of Zurich, Department of Economics, Working Paper. [12, 22, 23]
ROTHKOPF, MICHAEL H, THOMAS J TEISBERG, AND EDWARD P KAHN (1990): “Why are Vickrey auctions rare?” Journal of Political Economy, 98, 94–109. [1]
SATTERTHWAITE, MARK A AND HUGO SONNENSCHEIN (1981): “Strategy-proof allocation mechanisms at differentiable points,” The Review of Economic Studies, 48, 587–597. [4, 21]
SHAPLEY, LLOYD AND HERBERT SCARF (1974): “On cores and indivisibility,” Journal of Mathematical Economics, 1, 23–37. [12]
SONMEZ, TAYFUN AND M UTKU ÜNVER (2010): “Course bidding at business schools,” International Economic Review, 51, 99–123. [13]
THOMPSON, WILLIAM (2014): “Non-bossiness,” Rochester Center for Economic Research, Working Paper Number 586. [21]
VICKREY, WILLIAM (1961): “Counterspeculation, auctions, and competitive sealed tenders,” The Journal of Finance, 16, 8–37. [1, 14]
WALRAS, LEON (1874): Éléments D’economie Politique Pure. [18]
WILSON, ROBERT (1989): “Game Theoretic Analysis of Trading,” in Advances in Economic Theory: Fifth World Congress, CUP Archive, 12, 33. [14]
ONLINE APPENDIX

APPENDIX A: TÀTONNEMENT AND STABILITY, WITH AND WITHOUT MULTI-COUNT QUERIES

This section has two key results. First, we show that when the designer has access to only individual elicitation queries and count queries, the designer cannot contextually privately implement a stable school assignment rule. Then we show that when the designer can additionally use multi-count queries, it can implement a stable assignment rule with a tâtonnement (and thus contextually private) protocol.

We begin first with the impossibility under count queries alone.

**Proposition 11:** Assume that there are at least two agents and objects, agents have scores $s_i$, and there is no oversupply. There is no stable and contextually private choice rule for school assignment under individual elicitation queries and count queries.

**Proof:** Assume there was a contextually private protocol $P$ that uses only individual elicitation queries and count queries.

We consider type profiles in which students $i = 3, 4, \ldots n$ are assigned to schools. As we assume no oversupply, a partition where all but two colleges, which we call $a$ and $b$ have exactly as many students assigned as their capacity is. Assume that assigned students list the school as their highest priority, and that all other students have low scores at the school. Assume that agents 1 and 2 each have school $a$ as their most preferred school. Assume that $s_1 > s'_2 > s'_1 > s_2$ are scores at school $a$, which are lower than all other students’ scores at $a$. We consider four different type profiles for the scores at school $a$:

1. Agent 1 has score $s_1$, Agent 1 has score $s_2$;
2. Agent 1 has score $s'_1$, Agent 2 has score $s_2$;
3. Agent 1 has score $s_1$, Agent 1 has score $s'_2$;
4. Agent 1 has score $s'_1$, Agent 1 has score $s'_2$.

Note that in these type profiles, stability demands that the first three type profiles lead to an assignment of agent 1 to school $a$ and agent 2 to school $b$; the last needs to assign student 1 to school $b$ and student 2 to school $a$. Hence, there must be a node separating these type profiles. We show that for any query $A$ that separates these types, there is a violation of contextual privacy.

**Case 1:** $A$ is a sequential elicitation query. Without loss, consider the case that a sequential elicitation query to agent 1 is asked. This separated type profiles $\{(1), (3)\}$ from $\{(2), (4)\}$. Note that type profiles 1 and 2 only differ in the type of agent 1 and lead to the same outcome, which is a contradiction to contextual privacy.

**Case 2:** $A$ is a count query. In this case, the following is an exhaustive list of partitions that can be reached through counting queries, which we list with their potential predicates. Note that this list can be obtained by considering all 16 possible subsets of $\{s_1, s_2, s'_1, s'_2\}$. Observe that $\Theta = \emptyset$ and $\Theta = \{s_1, s_2, s'_1, s'_2\}, \Theta = \{s_1, s'_1\}$, and $\Theta = \{s_2, s'_2\}$ are unable to separate the types from 1 to 4.

- $\{(1), (2)\}, \{(3), (4)\}$ (for $\Theta \in \{\{s_1, s'_1, s_2\}, \{s_1, s'_2\}, \{s_1\}, \{s'_1\}\}$);
- $\{(1), (3)\}, \{(2), (4)\}$ (for $\Theta \in \{\{s_1, s_2, s'_2\}, \{s'_1, s_2, s'_2\}, \{s_1\}, \{s'_1\}\}$);
- $\{(1), \{2\}, \{3\}, \{4\}$ (for $\Theta \in \{\{s_1, s_2\}, \{s'_1, s'_2\}\}$)
- $\{(3)\}, \{(1), (4)\}, \{(2)\}$ (for $\Theta \in \{\{s_1, s'_2\}, \{s'_1, s_2\}\}$)

In the first, third and fourth case, type profiles 1 and 3 are separated, lead to the same outcome, and only differ in agent 2’s type, hence contradict contextual privacy. In the second case, type
profiles 1 and 2 are separated, lead to the same outcome, and only differ in agent 1’s type. Hence, in any case, we arrive at a contradiction to contextual privacy.

Hence, for any possible query separating any of the types \((1), (2), (3), (4)\) from any of the other possible profiles, a violation of contextual privacy results. As such separation is needed to certify a stable choice rule, a contextual private implementation is not possible under count queries and individual elicitation queries.

Q.E.D.

We next show that there is a contextually private protocol that uses only individual elicitation queries and multi-count queries that produces a stable outcome for the school assignment problem. This proof requires assuming that the cutoff is part of the social outcome.

**Definition**—Multi-count query: A query for node \(v\) is a *multi-count query* if there are sets \(\tilde{\Theta}^{(1)}_v, \tilde{\Theta}^{(2)}_v, \ldots, \tilde{\Theta}^{(l)}_v \subseteq \Theta\) such that for \((v, w) \in E\),

\[
\Theta_w = \{ \theta \in \Theta_v : (|\{i \in N : \theta_i \in \tilde{\Theta}^{(i)}_v\}|)_{i=1,2,\ldots,l} \in A \},
\]

for some \(A \subseteq \{1, 2, \ldots, n\}^l\).

**Proposition 12:** There is a contextually private protocol producing a stable outcome under multi-count queries if cutoff scores are part of the outcome.

**Proof:** Recall that in the auction domains, types are \(\theta_i = (\prec_i, s_i)\) consisting of a preference order on schools and scores \(s_i\). We prove the statement by giving a tâtonnement protocol that produces a stable outcome. The protocol starts with the binary queries asking for market clearing for any cutoff vector \(\sigma\), with children \(\{\Theta : |\{i \in N : \max_{\prec_i} \{j : s_i \geq \sigma_j\}\} | \leq \kappa(c)\}, \) for all \(c \in C\) (9)

and

\[
\{\Theta : |\{i \in N : \max_{\prec_i} \{j : s_i \geq \sigma_j\}\} | > \kappa(c)\}, \) for some \(c \in C\}
\]

for any ordering on score cutoffs \(\sigma\).

The first time (9) holds, agents are asked to sequentially choose a school from the schools with remaining places that they have been admitted to. Observe that this algorithm leads to a stable outcome. An agent cannot envy an admitted agent of a lower score, as admission is determined by scores.

It remains to show that the protocol is tâtonnement. It is straightforward to observe that the second phase of this algorithm is contextually private. It remains to show that the first phase results in distinct outcomes. Hence consider two cutoff profiles \(\sigma, \sigma'\) and two type profiles \(\theta\) and \(\theta'\) such that under \(\theta\), the market for \(\sigma\) clears, and for \(\theta'\) the market for \(\sigma'\) but not for \(\sigma\) clears. Under the assumption that cutoff scores are part of the outcome it is clearly the case that outcomes in different queries at the end of the first phase are disjoint, as they lead to different cutoff scores.

Q.E.D.

**Appendix B: Group Contextual Privacy and Obvious Strategyproofness**

The following example illustrates that there are rules that are group contextually private but not obviously strategyproof.
EXAMPLE—Non-Clinching Rule: In particular, there are strategyproof choice rules that are not obviously strategyproof but group-contextually private. As an example, consider \( n = 2 \), \( \Theta = \{\theta, \bar{\theta}\} \) and \( \mathcal{X} = \{x_1, x_2, x_3, x_4\} \). Assume that for agent 1,

\[
x_1 \succ_\theta x_3 \succ_\theta x_2 \succ_\theta x_4
\]

\[
x_1 \prec_\theta x_3 \prec_\theta x_2 \prec_\theta x_4
\]

and for agent 2

\[
x_1 \succ_\theta x_2 \succ_\theta x_3 \succ_\theta x_4
\]

\[
x_1 \prec_\theta x_2 \prec_\theta x_3 \prec_\theta x_4.
\]

Consider the social choice function

\[
\phi(\theta, \bar{\theta}) = x_1 \quad \phi(\bar{\theta}, \theta) = x_2 \quad \phi(\theta, \theta) = x_3 \quad \phi(\bar{\theta}, \bar{\theta}) = x_4.
\]

As the rule is injective, any protocol implementing it is group contextually private. It is also tedious but straightforward to check that this rule is strategyproof. There is no obviously strategyproof implementation, however. Assume that agent 1 is asked to play first. They face a choice between outcomes \( \{x_1, x_3\} \) and \( \{x_2, x_4\} \), which, for both \( \theta \) and \( \bar{\theta} \) types are are not ordered in the set order, and hence make no action obviously dominated. A similar observation for agent 2 shows that neither first action can be obviously dominant.

APPENDIX C: IMPOSSIBILITY OF SECOND-PRICE AUCTION CONTEXTUAL PRIVACY UNDER NO-TIES

We include the following alternative proof of Proposition 4 which does not rely on ties. While Brandt and Sandholm (2008) includes a proof analogous to the one in the main text using the Corners Lemma, they do not present a more general proof as the one below. Note that in order to guarantee that there are no ties, we assume that the type space has at least 9 values. As auctions are often studied in continuous type spaces, this is restriction is not too consequential.

ALTERNATE PROOF OF PROPOSITION 4 (NO TIES): This proof proceeds in two steps. First, we construct a direct contradiction of Proposition 1 in a case with \( n = 3 \) and \( |\Theta| = 9 \). Then we argue that for any auction with \( n \geq 3 \) and \( |\Theta| \geq 9 \), this counterexample cannot be ruled out.

Construction of a minimal counterexample. Let \( n = 3 \) and let

\[
\Theta = \{\theta_0, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7, \theta_8\}.
\]

Consider the product set \( \Theta' = \{\theta_5, \theta_0, \theta_2\} \times \{8, 7, 3\} \times \{6, 4, 1\} \). In this product set, the first factor represents types of agent 1, the second represents possible types of agent 2, and the third represents possible types of agent 3. We will show that when \( \phi_{SPA} \) is evaluated on this restricted product set, it is non-constant and all types in the product set are inseparable.

To see this, we construct the tensor of outcomes for the product set. This tensor is represented in Figure C.1. We represent agent 1’s type on the up-down axis, agent 2’s type on the left-right axis, and agent 3’s type is constant for each box. The outcomes under \( \phi_{SPA} \) are represented by letters and colors. For example, the upper left corner in the left-most box signifies \( \phi_{SPA}(\theta_2, \theta_8, \theta_6) = a \), where \( a \) is the outcome under which agent 2 wins the object and pays a price \( \theta_6 \)
To see that this constitutes a violation of contextual privacy, we show that: (i) \( \phi \) is non-constant on \( \Theta' \), and (ii) for all agents \( i \), and all \( \theta_i, \theta_i' \in \Theta' \), \( \theta_i \) and \( \theta_i' \) are inseparable. As for (i), we can observe immediately that \( \phi|_{\Theta'} \) is non-constant. To see (ii) that all types are inseparable, we go through each agent in turn.

- **Agent 1**: Outcome \( a \) is the same for \( \theta_{-1} = (\theta_7, \theta_6) \), hence all agent 1 types are inseparable.
- **Agent 2**: Outcome \( i \) for \( \theta_{-2} = (\theta_5, \theta_1) \) show that all agent 2 types are inseparable.
- **Agent 3**: \( \theta_6 \) and \( \theta_4 \) are inseparable because they both yield outcome \( b \) for \( \theta_{-3} = (\theta_0, \theta_3) \).

\( \theta_1 \) and \( \theta_4 \) are inseparable because they both yield outcome \( d \) for \( \theta_{-3} = (\theta_2, \theta_7) \).

Now that we have constructed a counter-example, we argue that for any settings with \( n \geq 3 \) and \( |\Theta| \geq 9 \), this situation cannot be ruled out. Consider a restriction \( \Theta'' = \Theta' \times \prod_{i \in \{4, \ldots, n\}} \Theta_i \) where each \( \Theta_i \), for agents \( i \in \{4, \ldots, n\} \) contains only types below \( \theta_9 \) and \( \Theta' \) is as defined in step 1. Then, \( \phi|_{\Theta''} = \phi|_{\Theta'} \). As shown in step 1, \( \phi|_{\Theta'} \) is non-constant and all types are inseparable.

Q.E.D.