Online Appendix

Proof of Lemma 3

We prove Lemma 3 by proving a more general result, as stated below.

Lemma OA.1. *Consider any statistic* $\phi : \Omega \to \mathbb{R}$*. Let* $\mathcal{D}_\phi$ *be the collection of distributions* $\rho \in \Delta(\mathbb{R}^J)$ *such that the marginal of the* j*-th component equals* $F_\phi(\cdot \mid \theta_j)$*. Then,* $\rho \in \Delta(\mathbb{R}^J)$ *is the joint distribution of* $(F_\phi^{-1}(M_{\theta_j}(s)) \mid \theta_j)_{j=1}^J$ *for the* $(M_{\theta_j})_{j=1}^J$*-reordered* ϕ*-quantile signal if and only if* $\rho \in \mathcal{D}_\phi$*.*

Proof. Consider any family $M = (M_{\theta_j})_{j=1}^J$ of measure-preserving transformations. Since s is uniformly distributed, the distribution of $F^{-1}(M_{\theta_j}(s) \mid \theta_j)$ is $F(\cdot \mid \theta_j)$ for all $j \in \{1, \dots, J\}$. Therefore, the joint distribution ρ of $(F^{-1}(M_{\theta_j}(s) \mid \theta_j))_{j=1}^J$ is in $\mathcal{D}_\phi$.

Conversely, consider any $\rho \in \mathcal{D}$. Since Ω^J is standard Borel, there exists measurable functions $\{\eta_j\}_{j=1}^J$ such that the joint distribution of $(\eta_j(s))_{j=1}^J$ is ρ, where s is a uniform random variable on $[0,1]$. Since for all $j \in \{1, \dots, J\}$, $\eta_j(s)$ and $F^{-1}(s \mid \theta_j)$ have the same distribution, there exists a measure-preserving transformation $M_{\theta_j} : [0,1] \to [0,1]$ such that $\eta_j(\hat{s}) = F^{-1}(\Phi_{\theta_j}(\hat{s}) \mid \theta_j)$ for all $\hat{s} \in [0,1]$ and for all $j \in \{1, \dots, J\}$ by Proposition 3 of Ryff (1970), as desired. $\square$

With Lemma OA.1, Lemma 3 follows immediately by taking ϕ to be a Borel isomorphism.

Proof of Proposition 2

We prove Proposition 2 by proving a more general result, stated as follows.

Proposition OA.1. *For any statistic* $\phi : \Omega \to \mathbb{R}$*, and for any decision problem* (u, A) *with* $u(\omega, a) = h(\phi(\omega), \theta(\omega), a)$*, let*

$$\widetilde{V}(x_1, \dots, x_J) := \sup_{a \in A} \left(\sum_{j=1}^J h(x_j, \theta_j, a) \mathbb{P}[\theta = \theta_j] \right), \tag{A.8}$$

for all $(x_j)_{j=1}^J \in \mathbb{R}^J$*. Then, the decision-maker's optimal value* $V^\star$ *among all privacy-preserving* *signals for* (ϕ, θ) *is given by*

$$V^\star = \sup_{\rho \in \mathcal{D}_\phi} \int_{\mathbb{R}^J} \widetilde{V}(x_1, \dots, x_J)\, \mathrm{d}\rho\,. \tag{A.9}$$

Moreover, any optimal privacy-preserving signal must be Blackwell-equivalent to some M*-reordered* ϕ*-quantile signal such that the distribution of* $(F_\phi^{-1}(M_{\theta_j}(s) \mid \theta_j))_{j=1}^J$ *is a solution of* (A.9).

Proof. By Proposition A.1 and Blackwell's theorem, any privacy-preserving signal for (ϕ, θ) yields a (weakly) lower payoff to the decision-maker than some reordered ϕ-quantile signal. Together with Lemma OA.1, it then follows that

$$V^\star = \sup_{\rho \in \mathcal{D}_\phi} \int_{\mathbb{R}^J} \widetilde{V}(x_1, \dots, x_J)\, \mathrm{d}\rho\,.$$

Moreover, by Proposition A.1, any privacy-preserving for (ϕ, θ) that yields $V^\star$ must be the M-reordered ϕ-quantile signal s, for some family $M = (M_{\theta_j})_{j=1}^J$ of measure-preserving transformations. Thus, by Lemma OA.1, the joint distribution of $(F_\phi^{-1}(M_{\theta_j}(s), \theta_j))_{j=1}^J$ must be a solution of (A.9). □

With Proposition OA.1, Proposition 2 follows immediately by taking ϕ as a Borel isomoriphism.

Proof of Proposition 3

Let $\widehat{V} : \mathbb{R}^J \times A \to \mathbb{R}$ be defined as

$$\widehat{V}(x_1, \dots, x_J, a) := \sum_{j=1}^J h(x_j, \theta_j, a) \mathbb{P}[\theta = \theta_j].$$

We first show that $\widehat{V}$ has increasing difference in $(x_1, \dots, x_J)$ and a, and is supermodular in $(x_1, \dots, x_J)$. Indeed, for any $a, a' \in A$ and $\mathbf{x} = (x_j)_{j=1}^J, \mathbf{x}' = (x'_j)_{j=1}^J \in \Omega^J$ such that $a \geq a'$ and

$x_j \geq x'_j$ for all j,

$$\begin{aligned}\widehat{V}(\mathbf{x}, a) - \widehat{V}(\mathbf{x}, a') &= \sum_{j=1}^{J} [h(x_j, \theta_j, a) - h(x'_j, \theta_j, a')] \mathbb{P}[\theta = \theta_j] \\ &\geq \sum_{j=1}^{J} [h(x'_j, \theta_j, a) - h(x'_j, \theta_j, a')] \mathbb{P}[\theta = \theta_j] \\ &= \widehat{V}(\mathbf{x}', a) - \widehat{V}(\mathbf{x}', a'),\end{aligned}$$

where the inequality follows from the supermodularity of h. Furthermore, for any $\mathbf{x} = (x_j)_{j=1}^{J}, \mathbf{x}' = (x'_j)_{j=1}^{J} \in \Omega^J$ and for all $a \in A$,

$$\begin{aligned}\widehat{V}(\mathbf{x} \vee \mathbf{x}', a) + \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a) &= \sum_{j=1}^{J} [h(\max\{x_j, x'_j\}, \theta_j, a) + h(\min\{x_j, x'_j\}, \theta_j, a)] \mathbb{P}[\theta = \theta_j] \\ &= \sum_{j=1}^{J} [h(x_j, \theta_j, a) + u(x'_j, \theta_j, a)] \mathbb{P}[\theta = \theta_j] = \widehat{V}(\mathbf{x}, a) + \widehat{V}(\mathbf{x}', a).\end{aligned}$$

We next show that $\widetilde{V} : \Omega^J \to \mathbb{R}$ defined in (A.8) is supermodular. Since $\operatorname{argmax}_{a \in A} \widehat{V}(\mathbf{x}, a)$ is nonempty for all $\mathbf{x} \in \Omega^J$, for any $a^\star(\mathbf{x}) \in \operatorname{argmax}_{a \in A} \widehat{V}(\mathbf{x}, a)$ and for any $\mathbf{x} = (x_j)_{j=1}^{J} \in \mathbb{R}^J$, $\widetilde{V}(\mathbf{x}) = \widehat{V}(\mathbf{x}, a^\star(\mathbf{x}))$. Therefore, it suffices to show that

$$\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) + \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) \geq \widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}')),$$

for all $\mathbf{x}, \mathbf{x}' \in \Omega^J$, and for any selection $a^\star(\cdot)$ for the argmax correspondence. To see this, consider any $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^J$ and any selection $a^\star(\cdot)$. Since A is totally ordered, it is without loss to assume that $a^\star(\mathbf{x}) \geq a^\star(\mathbf{x}')$. As a result,

$$\begin{aligned}
&\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) + \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')))\\
=&\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}))\\
&+ [\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) - \widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x}))] + [\widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}))]\\
\geq&\widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}))\\
&+ [\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) - \widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x}))] + [\widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}))]\\
=&\widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}')) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x})) - \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}'))\\
&+ [\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) - \widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x}))] + [\widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}))]\\
\geq&\widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}')) + \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x})) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}'))\\
&+ [\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) - \widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x}))] + [\widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}))]\\
=&\widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}'))\\
&+ [\widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x} \vee \mathbf{x}')) - \widehat{V}(\mathbf{x} \vee \mathbf{x}', a^\star(\mathbf{x}))] + [\widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x} \wedge \mathbf{x}')) - \widehat{V}(\mathbf{x} \wedge \mathbf{x}', a^\star(\mathbf{x}'))]\\
\geq&\widehat{V}(\mathbf{x}, a^\star(\mathbf{x})) + \widehat{V}(\mathbf{x}', a^\star(\mathbf{x}'))\,,
\end{aligned}$$

where the first inequality follows from supermodularity of $\widehat{V}$, the second inequality follows from the increasing difference property of $\widehat{V}$ and from $a^\star(\mathbf{x}) \geq a^\star(\mathbf{x}')$, and the third inequality follows from optimality of $a^\star$.

Now let

$$\widetilde{V}(\mathbf{x}) := \sup_{a \in A} \widehat{V}(\mathbf{x}, a) = \sup_{a \in A} \sum_{j=1}^{J} h(x_j, \theta_j, a)\mathbb{P}[\theta = \theta_j]\,,$$

for all $\mathbf{x} \in \mathbb{R}^J$. Note that by Lemma OA.1, (A.9) is equivalent to choosing a family $(M_j)_{j=1}^J$ of measure-preserving transformations to maximize

$$\int_0^1 \widetilde{V}(F_\phi^{-1}(M_1(q) \mid \theta_1), \dots, F_\phi^{-1}(M_J(q) \mid \theta_J))\,\mathrm{d}q\,.$$

Since $\widetilde{V}$ is supermodular, Theorem 5 of Tchen (1980) (see also, Theorem 2.1 of Puccetti and Wang 2015) implies that

$$\int_0^1 \widetilde{V}(F_\phi^{-1}(M_1(q) \mid \theta_1), \dots, F_\phi^{-1}(M_J(q) \mid \theta_J))\,\mathrm{d}q \leq \int_0^1 \widetilde{V}(F_\phi^{-1}(q \mid \theta_1), \dots F_\phi^{-1}(q \mid \theta_J))\,\mathrm{d}q$$

for any family $(M_j)_{j=1}^J$ of measure-preserving transformations. Together with Proposition OA.1, $V^\star$ is attained by the ϕ-quantile signal, as desired. $\square$

Proof of Proposition 6

For any $\rho \in \mathcal{D}$, Lemma 3 implies that there exists a family $M = (M_{\hat{\theta}})_{\hat{\theta}\in\Theta}$ of measure-preserving transformations such that the joint distribution of $(\tilde{\omega}_j^M)_{j=1}^J$ is ρ. Consider the problem where the sender is restricted to choose garblings of the M-reordered ϕ-quantile signal, for some conditionally revealing ϕ-quantile signal. Standard arguments (Kamenica and Gentzkow 2011) imply that the sender's value in this restricted problem is $\overline{V}_S(\rho)$. By Theorem 1, since every privacy-preserving signal is a garbling of some reordered ϕ-quantile signal, the sender's value $V_S^\star$ in the original problem must be given by

$$\max_{\rho\in\mathcal{D}} \overline{V}_S(\rho)\,. \qquad \square$$

Proof of Proposition 10

Consider the market segmentation that corresponds to the quantile signal q. Under this segmentation, there is a continuum of segments $\hat{q} \in [0,1]$, and in each segment $\hat{q} \in [0,1]$, there are J possible consumer values $\{F^{-1}(\hat{q} \mid \theta_j)\}_{j=1}^J$. Let $\rho^\star \in \mathcal{D}$ be the joint distribution of $\{F^{-1}(q \mid \theta_j)\}_{j=1}^J$.

We now show that $\rho^\star$ solves the optimal transport problem (6). To this end, we construct the Lagrange multipliers such that weak duality holds under $\rho^\star$. Let $K_1(x_1) := x_1$, and let $K_j(x_j) := 0$ for all $j \in \{2,\dots,J\}$. Then, since $F(\cdot \mid \theta_1) \geq \dots \geq F(\cdot \mid \theta_J)$, $x_1 \leq \dots, x_J$ for all $(x_j)_{j=1}^J \in \operatorname{supp}(\rho^\star)$. Moreover, since $(1-\mathbb{P}[\theta=\theta_1])\cdot\overline{x} \leq \underline{x}$, $V(x_1,\dots,x_n) = x_1$ for all $(x_j)_{j=1}^J \in \operatorname{supp}(\rho^\star)$. Therefore,

$$\sum_{j=1}^J K_j(x_j) = x_1 = V(x_1,\dots,x_J)\,,$$

for all $(x_j)_{j=1}^J \in \operatorname{supp}(\rho^\star)$.

Meanwhile, for any $(x_j)_{j=1}^J \in [\underline{x},\overline{x}]^J$, if $x_1 = \min\{x_j\}_{j=1}^J$, then $V(x_1,\dots,x_J) = x_1$. If $x_1 > \min\{x_j\}_{j=1}^J$, let $x_{(j)}$ denotes the (j)-th smallest element of $(x_j)_{j=1}^J \in [\underline{x},\overline{x}]^J$ and let

$(j) \in \{1, \ldots, J\}$ be the index of that element. Then,

$$x_1 \geq \underline{x} \geq (1 - \mathbb{P}[\theta = \theta_1])\overline{x} \geq \sum_{j=i}^{J} \mathbb{P}[\theta = \theta_{(j)}]\overline{x} \geq \sum_{j=i}^{J} \mathbb{P}[\theta = \theta_{(j)}]x_{(j)} \,,$$

for all $i \in \{2, \ldots, J\}$. Thus,

$$\sum_{j=1}^{J} K_j(x_j) = x_1 \geq \max_{i \in \{1,\ldots,J\}} \sum_{j=i}^{J} \mathbb{P}[\theta = \theta_{(j)}]x_{(j)} = V(x_1, \ldots, x_J) \,.$$

As a result, $\{K_j\}_{j=1}^J$ are the Lagrange multipliers that warrant $\rho^\star$ as a solution. This proves (i). (ii) through (iv) then follows immediately from the fact that $F^{-1}(\hat{q} \mid \theta_1) \leq F^{-1}(\hat{q} \mid \theta_j)$ for all $\hat{q} \in [0,1]$ and for all $j \in \{1, \ldots, J\}$. This completes the proof. □

Constructing a Reordered Quantile Signal

Consider any ϕ-quantile signal q_ϕ. Let $(M_{\hat{\theta}})_{\hat{\theta} \in \Theta}$ be a family of measure-preserving transformations such that $\hat{\theta} \mapsto M_{\hat{\theta}}(s)$ is measurable, for all $s \in [0,1]$. We now construct explicitly the M-reordered ϕ-quantile signal.

Let $\xi, \zeta : [0,1] \to [0,1]$ be two independent random variables that are uniformly distributed. Let

$$q := \xi F_\phi(\phi \mid \theta) + (1 - \xi) F_\phi^-(\phi \mid \theta) \,.$$

Then q is independent of ζ and is Blackwell-equivalent to q_ϕ. Fix any $\hat{\theta} \in \Theta$, and let $C_{\hat{\theta}}$ be the joint distribution of $(\zeta, M_{\hat{\theta}}(\zeta))$, i.e.,

$$C_{\hat{\theta}}(u, v) := \mathbb{P}[\zeta \leq u, M_{\hat{\theta}}(\zeta) \leq v] \,,$$

for all $u, v \in [0,1]$. Note that by definition $C_{\hat{\theta}}$ assigns probability one to the set $\{(u,v) \in [0,1]^2 : u = M_{\hat{\theta}}(v)\}$

Let $K_{\hat{\theta}} : [0,1] \to [0,1]$ be the disintegration (see, e.g., Çinlar 2010, Theorem 2.18, pp. 154) of $C_{\hat{\theta}}$ with respect to the Lebesgue measure, so that

$$C_{\hat{\theta}}(u, v) := \int_0^u K_{\hat{\theta}}(v \mid z) \, \mathrm{d}z \,.$$

Thus, for any random variable s that is distributed according to $K_{\hat{\theta}}(\cdot \mid \hat{q})$ conditional on $\hat{\theta}$ and $\hat{q}$,

$$\mathbb{P}[M_{\hat{\theta}}(s) = \hat{q} \mid \hat{\theta}, \hat{q}] = 1\,.$$

Thus, let

$$s := K_{\theta}^{-1}(\zeta \mid q)\,.$$

The distribution of s conditional on $\hat{\theta}$ and $\hat{q}$ is then $K_{\hat{\theta}}(\cdot \mid \hat{q})$. Therefore, almost surely,

$$M_{\theta}(s) = q\,,$$

which in turn implies that $M_{\theta}(s) \sim q_{\phi}$, as desired.

Furthermore, note that for any s such that $M_{\theta}(s) \sim q_{\phi}$, s must be Blackwell-equivalent to a signal $\tilde{s}$ that is distributed according to $K_{\hat{\theta}}(\cdot \mid \hat{q})$ conditional on $\hat{\theta}$ and $\hat{q}$, for almost all $\hat{\theta}$ and $\hat{q}$. Since the disintegration of $C_{\hat{\theta}}$ is essentially unique, it follows that a reordered ϕ-quantile signal is unique up to Blackwell equivalence.

Belief-Based Characterization of Privacy-Preserving Signals

For completeness, we provide a characterization of privacy-preserving signals in terms of distributions over posterior beliefs that is equivalent to Theorem 1. Denote by $p_0(A) := \mathbb{P}[\omega \in A]$ the probability of event $A \in \mathcal{F}$ under the prior.

Suppose that there are only finitely many states $|\Omega| < \infty$ and (without loss) that the privacy sets are disjoint: $P \cap P' = \varnothing$ for all $P, P' \in \mathcal{P}$. From Blackwell's theorem (Blackwell 1953), a signal s can be equivalently represented by a random variable $p : \Omega \to \Delta(\Omega)$ such that $\mathbb{E}[p] = p_0$. Therefore, a signal p is privacy-preserving if and only if

$$\begin{gathered} \mathbb{E}\left[p\right] = p_0 \\ \mathbb{P}\left[\sum_{\omega \in P} p(\omega) = \sum_{\omega \in P} p_0(\omega)\right] = 1 \qquad \forall P \in \mathcal{P}\,. \end{gathered} \tag{A.10}$$

Our results show that the Blackwell frontier of the set of privacy-preserving signals is given by those privacy-preserving signals which in addition satisfy

$$\mathbb{P}\left[|\text{supp}(p) \cap P| = 1\right] = 1 \qquad \forall P \in \mathcal{P}. \tag{A.11}$$

In other words, (A.10) holds if and only if p is a mean-preserving contraction of some $\tilde{p}$ which satisfies (A.10) and (A.11). For a general state space Ω, the characterization is similar.

Relaxing the Independence Criterion

An immediate implication of Remark 2 is a relaxation of the definition of privacy-preserving signals. While we define privacy-preserving signals by the notion of independence, conditionally privacy-preserving signals relax the independence requirement by allowing for correlations with the component y. In particular, one may consider a signal y that is independent of a statistic $\phi : \Omega \to \mathbb{R}$, but is not privacy-preserving.[38] Conditionally privacy-preserving signals in this environment can then be regarded as privacy-preserving signals with a less stringent requirement for posterior beliefs, as changes in posterior beliefs on privacy sets conditional on realizations of s would be allowed as long as it is through y.

Another Notion of Algorithmic Fairness

In §5.1, we show how our results can be applied to the literature of algorithmic fairness and demonstrate how privacy-preserving signals are related to the notion of fairness called independence. In the literature on algorithmic fairness, there are other notions of fairness that do not require statistical independence, as discussed in §5.1. One of the most commonly used alternatives to statistical independence is called *separation*. Separation requires the decisions to be independent of protected characteristics *conditional on the true state*.

Our results can also be applied to this setting. To see this, suppose that the underlying outcome, γ, is binary and takes values 0 or 1. Let x be the expected probability of the underlying state being $\gamma = 1$, conditional on all the observable covariates (including protected characteristics θ). A signal would satisfy the requirement of separation if its realization is independent of θ conditional on γ. Consider any conditionally privacy-preserving signal s. By

[38] In fact, we can fully characterize these signals, as they are equivalent to privacy-preserving signals for θ that are independent of ϕ.

definition, such a signal would be independent of θ conditional on γ. Moreover, a conditionally privacy-preserving signal is Blackwell-undominated if and only if it takes the form of (s, γ), where $\tilde{s}$ is some reordered quantile signal conditional on γ. Although the signal that reveals $(\tilde{s}, \gamma)$ may not be feasible, as the outcome γ is typically unknown, one can project this signal by computing the conditional expectation of $(\tilde{s}, \gamma)$ given x. This conditional expectation is thus, by construction, a garbling of x, and is conditionally independent of θ given γ. Furthermore, since taking the conditional expectation preserves the Blackwell order, this signal must remain Blackwell-undominated among all feasible signals.

Privacy-Preserving Segmentation and Uniform Pricing

Consider the following example demonstrating that high value consumers might be better-off under the seller-optimal privacy-preserving segmentation than under uniform pricing. Suppose that $X = [1/3, 1]$, $F(x \mid \theta_1) = 3/2(x - 1/3)$, $F(x \mid \theta_2) = 2(x - 1/2)^+$ for all $x \in X$, and $\mathbb{P}[\theta = \theta_1] = 1/3$, $\mathbb{P}[\theta = \theta_2] = 2/3$. The optimal uniform price is $4/5$, and the surplus of θ_2 consumers is $1/25$. Under the seller-optimal privacy-preserving segmentation, the surplus of θ_2 consumers is $1/12 > 1/25$.

Verifying the Optimality of $\rho^\star$

In Section 5.3, we claim that the joint distribution $\rho^\star$ is optimal in our example. To see this, recall that a joint distribution $\rho \in \mathcal{D}$ is a solution of the associated optimal transport problem if and only if there exists Lagrange multipliers $K_1, K_2 : \{1,2,3\} \to \mathbb{R}$ that satisfy the complementary slackness condition: $K_1(x_1) + K_2(x_2) \geq V(x_1, x_2)$, for all $(x_1, x_2) \in \{1,2,3\}^2$, with equality on the support of ρ. It can then be verified that the complementary slackness condition is satisfied under the Lagrange multipliers $(K_1(x))_{x \in \{1,2,3\}} = (1, 2, 5/2)$ and $(K_2(x))_{x \in \{1,2,3\}} = (0, 0, 1/2)$, and hence $\rho^\star$ is indeed a solution.