Online Appendix for: Why the Economics Profession Must Actively Participate in the Privacy Protection Debate

By JOHN M. ABOWD, IAN M. SCHMUTTE, WILLIAM N. SEXTON, AND LARS VILHUBER[*]

This document provides the online appendix to "*Why the Economics Profession Must Actively Participate in the Privacy Protection Debate*".

[*] Abowd, Sexton, and Vilhuber: U.S. Census Bureau, Washington, DC, USA and Cornell University, Ives Hall, Ithaca, NY, USA. Schmutte: U.S. Census Bureau and University of Georgia, Amos Hall, Athens, GA, USA. This research was partially funded through NSF Grant #1131848 (NCRN) and Alfred P. Sloan Foundation Grant G-2015-13903. The views expressed in this paper are those of the authors and not those of the U.S. Census Bureau or other sponsors.

Online Appendix

Suppose a Bayesian adversary wants to learn the record R belonging to individual i, from a confidential database, x. She has auxiliary information E that includes traditional identifiers (e.g., name and address) along with other variables that can be used to match against data published via differential privacy. The adversary has prior μ over the space of possible data vectors $\mathscr{D}$. A data custodian uses a bounded ε-differentially private mechanism M to publish output $M(x) = \omega$. Bounded differential privacy mechanisms treat the total number of records in the confidential database as public. Unbounded differential privacy mechanisms inject noise into the total record count as well. The algorithms under consideration for use with the 2020 Census are in the class of bounded differential privacy mechanisms. Upon observing ω and E, the adversary updates her beliefs about R, the record of an individual i, using Bayes law. By the law of total probability,

$$\mu(R = r|\omega, E) = \sum_{z \in \mathscr{D}} \mu(R = r, z|\omega, E)$$

Note that

$$\begin{aligned}
\mu(R = r, z|\omega, E) &= \frac{\mu(R = r, \omega, E|z)\mu(z)}{\mu(\omega, E)} \\
&= \frac{\mu(R = r, E|z)Pr[M(z) = \omega]\mu(z)}{\sum_{y \in \mathscr{D}} \mu(\omega, E|y)\mu(y)} \\
&= \frac{\mu(R = r, E|z)Pr[M(z) = \omega]\mu(z)}{\sum_{y \in \mathscr{D}} \mu(E|y)Pr[M(y) = \omega]\mu(y)},
\end{aligned}$$

where the second equality follows under the assumption that ω is conditionally independent from R and E given z. The probability of observing ω given z is completely determined by the coin flips of the mechanism. Hence,

$$\mu(R = r|\omega, E) = \frac{\sum_{z \in \mathscr{D}} \mu(R = r, E, z)Pr[M(z) = \omega]}{\sum_{y \in \mathscr{D}} \mu(E, y)Pr[M(y) = \omega]}.$$

Now consider a hypothetical counterfactual where the mechanism M does not use i's record, and the adversary knows it. Instead M runs on $\tilde{x} = x_{-i} \cup r_f$ the data vector in which i's record is removed from x and replaced by an arbitrary default record, r_f. In this case, the adversary's updated beliefs are:

$$\mu_{-i}(R = r|\omega, E) = \frac{\sum_{z \in \mathscr{D}} \mu(R = r, E, z)Pr[M(\tilde{z}) = \omega]}{\sum_{y \in \mathscr{D}} \mu(E, y)Pr[M(\tilde{y}) = \omega]}.$$

The notation μ_{-i} characterizes beliefs over $\tilde{x}$ derived from μ and knowledge that R has been removed and replaced by r_f. We conclude the following:

$$
\begin{aligned}
\frac{\mu(R=r|\omega,E)}{\mu_{-i}(R=r|\omega,E)} &= \frac{\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(z)=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(y)=\omega]}{\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(\tilde{z})=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&= \frac{\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(z)=\omega]/\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(\tilde{z})=\omega]}{\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(y)=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\le \frac{\sum_{z\in\mathscr{D}}\mu(R=r,E,z)e^{\varepsilon}Pr[M(\tilde{z})=\omega]/\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(\tilde{z})=\omega]}{\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(y)=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\text{(M is bounded ε-differentially private so $Pr[M(z)=\omega]\le e^{\varepsilon}Pr[M(\tilde{z})=\omega]$.)} \\
&= \frac{e^{\varepsilon}\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(\tilde{z})=\omega]/\sum_{z\in\mathscr{D}}\mu(R=r,E,z)Pr[M(\tilde{z})=\omega]}{\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(y)=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\text{(Factor out e^{ε}.)} \\
&= \frac{e^{\varepsilon}}{\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(y)=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\text{(The summations in the numerator ratio cancel out; i.e., the ratio equals 1.)} \\
&\le \frac{e^{\varepsilon}}{\sum_{y\in\mathscr{D}}\mu(E,y)e^{-\varepsilon}Pr[M(\tilde{y})=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\text{(M is bounded ε-differentially private so $Pr[M(y)=\omega]\ge e^{-\varepsilon}Pr[M(\tilde{y})=\omega]$.)} \\
&= \frac{e^{\varepsilon}}{e^{-\varepsilon}\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]/\sum_{y\in\mathscr{D}}\mu(E,y)Pr[M(\tilde{y})=\omega]} \\
&\text{(Factor out $e^{-\varepsilon}$)} \\
&= e^{2\varepsilon} \\
&\text{(The summations in the denominator ratio cancel out; i.e., the ratio equals 1.)}
\end{aligned}
$$

Similarly, $\frac{\mu(R=r|\omega,E)}{\mu_{-i}(R=r|\omega,E)} \ge e^{-2\varepsilon}$.

Source code for Figure 1

```
\begin{center}
    \captionsetup{type=figure}
                \begin{tikzpicture}
                \small
                \color{black}
                \begin{axis}[
                        % axis lines middle,
                        xmin = 0,
                        xmax = 5,
                        domain = 0:5,
                        ymin=0,
                        ymax=1,
                        samples=100,
                        xlabel = {Privacy Loss ($\varepsilon$)},
            ylabel near ticks,
            xlabel near ticks,
            ylabel = {Accuracy},
                        xtick={0,  10},
                        xtick pos=left,
                        ytick pos=left
                        ]
                        % \addplot[blue, ultra thick] (x, 0.3*ln(x + (1+x^2)^(.5)));
                        \addplot[blue, ultra thick] (x,(1-e^(-x)));
                        \addplot[black, ultra thick, dashed, domain = 1.75:4] (x,.800852 + .049787068*x);
                        \addplot[black, ultra thick, dotted, domain = 0.05:1] (x,.090204 + 0.60653066*x);
                        \addplot[mark = *] coordinates{(0.5, 0.393469)} node[pin=0:{Data Custodians}]{};
                        \addplot[mark = *] coordinates{ (3,0.950213)} node[pin=268:{Data Users}]{};
                  \end{axis}
                \end{tikzpicture}
\caption{The trade-off between privacy loss and accuracy in data publication}
\label{fig:tradeoff}
\end{center}
```

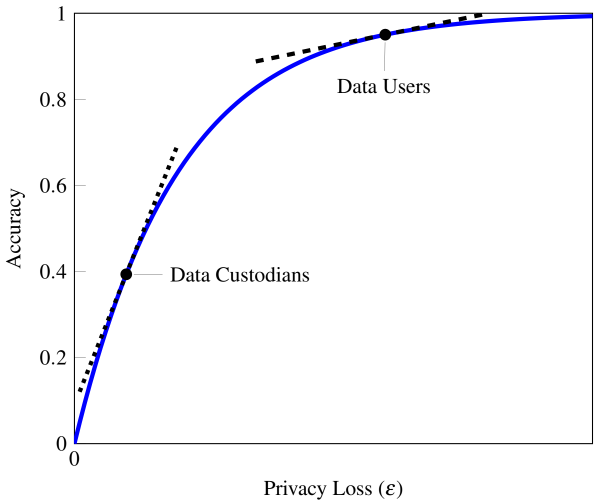

Figure B1. : The trade-off between privacy loss and accuracy in data publication