The Network Effect of Privacy Choices

Arthi Ramachandran and Augustin Chaintreau
Computer Science Department, Columbia University, New York NY, USA
arthir@cs.columbia.edu, augustin@cs.columbia.edu

1. INTRODUCTION

With most of their news, media and information coming from online social sources, users often personalize their information to receive better quality content. Most online services explicitly rely on data or actions from yourself and your friends for their service, or as training data or examples used for personalization. They also implicitly use this data for additional profit, which is typically perceived as an erosion of the user’s privacy. Any innocuous choice that is exercised online can reveal a lot of information about the individual. Indeed, with the explosion of data science techniques, the privacy risks involved with personalized information online are ever increasing. Unfortunately, navigating this trade-off today remains an uncertain endeavor. Among the difficulties is the formidable technical complexity of grasping how different data together can integrate to reveal, to different degrees of certainty, private information about the user.

Here, we wish to study a relatively under explored avenue of research: How does the disclosure of multiple types of data by locally connected individuals affect each one’s privacy differently? When and why can we expect that decisions made individually lead to predictable outcome? When are we likely to observe excessive privacy behaviors which appear seemingly irrational [1, 2] - such as refusing to disclose any data, or sharing most of your life? While this paper will consider a simple case the issue at stake is pervasive. Using vocabulary from micro-economics [8], while the enjoyment of your privacy through piece of mind or protection from future harm may appear as a conventional (i.e. private) utility, the enjoyment of personalization and social network sharing is by definition a public good. The quality of personalization (at the expense of privacy) highly depends on your connections and their individual choices.

In this paper, we present the following contributions:

- Inspired by a recent game theoretical analysis of a population estimate [8], we introduce the local wage poll, a natural extension of this problem to understand how social connections affect quality of estimation when information comes at a privacy cost. (Section 2)

- We prove that introducing an underlying graph in the estimation has a dramatic effect on the possible outcomes of this game. While a unique Nash equilibrium emerge in the previous case (similar to a complete graph), multiple outcomes are in general, possible, even in the simplest symmetric graphs. Examples abound where a subset of nodes lose most of their privacy, while others free-ride and enjoy convenience of knowledge at a lower cost. (Section 3)

- To understand this polarization phenomenon, we obtain an implicit form of the best response function. It allows us to reuse prior public good analysis and derive a sufficient condition ensuring that networks lead to single equilibrium that are generally less polarized. Interestingly this condition depends on the topology of the underlying network, specifically the graphs minimum eigenvalue. (Section 4)

It is well known that privacy has a social component. Some might even argue that privacy loss is “contagious”. It is also known that privacy often is a self-interested choice in the face of multiple alternatives[12, 11, 9]. But to our knowledge, there is relatively little work analyzing how the graph connecting individuals affect their privacy choices. Information privacy analyzed as a public good is a relatively new modeling technique [14]. The work which is the foundation of our model is a model of a global public good in which an estimate over an entire population is affected by individual choices [8]. Previous models of surveys with privacy costs make the same assumption [16, 13, 17]. Similarly, other related work focuses typically on large system in which an individual information disclosure affects the system only marginally [15, 18]. We show that, in sharp contrast, when information disclosed has a local effect, ensuring an efficient elicitation of private information can be much more difficult. On the other hand, we show that for the most privacy sensitive information, and in different types of graph, the predictable behavior of a centralized system can be reproduced. Those results are encouraging, especially as they allow to reuse the large set of theory introduced for the analysis of public good[5, 6, 3, 10, 4].

2. LOCAL WAGE POLL PROBLEM

Motivation: In a “local wage problem” we assume that a group of individuals are interested in computing the average wage in their vicinity or social neighborhood, without fully disclosing what they earn to their friends or in fact anyone else. We will consider a simple version of the game where wages are not dependent on your position in the network, and follows for each player the same distribution. There is a trusted authority (e.g., a Facebook app) which aggregates your information with the information from your friends to estimate your local average wage. We assume here, that
due to the private nature of the information, nobody is willing to disclose any information except to their friends. The presence of a centralized authority enforces users to commit to the values that they have given to the system. If each individual sets their own privacy level that they are comfortable with, how does each i still obtain a reasonable estimate?

**Notation:** We consider a set of N agents connected by social graph $G(N,E)$. Reusing notation from [8] we denote the global average salary $y_M$. Each agent has a (private) variable $y_i = y_M + e_i$ where $e_i$ is an i.i.d random variable with zero mean and variance $\sigma^2$. Each agent perturbs their variable before releasing it to their neighbors: $\bar{y}_i = y_i + z_i$ where $z_i$ is a zero mean random variable with a chosen variance $\sigma_i^2$. We use the precision $\lambda_i = \frac{1}{\sigma^2} \in [0, \frac{1}{\sigma^2}]$ as an aggregate measure of variance.

An agent, $i$, then makes an estimate based only on the values shared by her neighbors. Thus her estimate is: $\hat{y}_i(\lambda) = \frac{\lambda_i y_i + \sum_{j \in N(i)} \lambda_j y_j}{\lambda_i + \sum_{j \in N(i)} \lambda_j}$ As in the previous model, the estimator is unbiased. We denote $\lambda_{-i} = \sum_{j \in N(i)} \lambda_j$ as the precision of the neighbors of i. The variance of the estimator is $\sigma_i^2(\lambda) = \frac{1}{\lambda_i + \lambda_{-i}} \in \left[\frac{1}{\sigma^2}, \infty\right]$ where $d = |N(i)|$.

For any agent, their cost is split into two components: the privacy cost and the estimation cost. Each agent wishes to minimize their cost function $J_i(\lambda) = c\lambda_i^k + \sigma_i^2\lambda_i(\lambda)$ where $c > 0, k \geq 2$

$$J_i(\lambda) = c\lambda_i^k + \frac{1}{\lambda_i + \lambda_{-i}}. \quad (1)$$

**Best Response:** We analyze a single individual response of a player based on his neighbors privacy levels.

**Theorem 1.** For an agent i of graph $G(V,E)$, the best response function $\phi(\lambda_{-i}) = \lambda_i : \mathbb{R}^+ \rightarrow \mathbb{R}^+$, is given by the solution of $\lambda_{i, \star}^{k-1} = \frac{1}{\lambda_i + \lambda_{-i}}$.

**Proof.** For an individual, i, their best response occurs when cost is minimized w.r.t. the privacy level $\lambda_i$ chosen:

$$\min_{\lambda_i} J_i(\lambda) \text{ s.t. } \lambda_i \in [0, \frac{1}{\sigma^2}].$$

Hence, $\frac{dJ_i(\lambda)}{d\lambda_i} = 0,$

$$ck\lambda_i^{k-1} - \frac{1}{(\lambda_i + \lambda_{-i})^2} = 0,$$

$$\lambda_{i, \star}^{k-1} = \frac{1}{\sqrt{ck}}.$$

It is easy to see that the second derivative is positive and this is hence, a minimum point.

This implicit form admits no general explicit expression, except in the simple case where privacy cost is convex with a linear marginal cost (i.e., $k = 2$). The following simple corollary is obtained by substituting for $k = 2$.

**Corollary 2.** Assuming $k = 2$, $\phi(\lambda_{-i}) = \lambda_i^2$ where

$$r_i = \frac{2^2 \sqrt{\pi \lambda_{-i}} - (\sqrt{\pi} \sqrt{8c^3 \lambda_{-i}^2 + 27 \pi^2 - 9\pi^2 \lambda_{-i}^2})^{\frac{1}{2}}}{6^{\frac{1}{2}} \sqrt{\pi}}.$$

Figure 1 examines the behavior of the best response function under different conditions for a fixed $k = 2$. Similar qualitative trends can be found for any value of $k$. The best response function $\phi$ is decreasing in either $\lambda_{-i}$ or $c$ when the other is fixed.

**Symmetric graph:** While the analysis of Nash Equilibrium is left for a later section, we immediately observe that in a simple case ($d$-regular graph for any $d$), one can immediately deduce that a symmetric Nash Equilibrium exists.

**Claim 3.** For a $d$-regular graph, a symmetric Nash Equilibrium always exists and is given by $\lambda^* = \left(\frac{1}{(d+1)^{d+2}}\right)^{\frac{1}{d+1}}$.

**Proof.** Let $\lambda_i = \lambda^*, \forall i \in N$.

$$\lambda^{k-1}(\lambda^* + d \cdot \lambda^*)^2 = \frac{1}{ck} \implies \lambda^* = \left(\frac{1}{(d+1)^{d+2}}\right)^{\frac{1}{d+1}}$$

In such situation, a fortiori if one can prove that this equilibrium is unique, then we could expect a local wage poll to reproduce locally all the properties of a global private poll among $(d+1)$ participants.

3. **POLARIZATION**

In an ideal scenario, the equilibrium that results from such a game would be balanced i.e., agents contribute information roughly equally. In a balanced situation, there are no free-loaders to reveal very little information while using their neighbors information. To examine if this is indeed the case, we use simulations to further characterize the Nash Equilibrium in different graph families. We numerically compute the Nash Equilibrium using an iterative update algorithm.

In each update, we numerically solve for the best response of the implicit function. These can be later verified to be equilibria by checking that they satisfy the best response equations. Figure 2 shows the privacy levels in the Nash Equilibrium for complete, star, cycle and bipartite graphs of varying sizes. These illustrated simple graphs are symmetric so the expectation is that the Nash Equilibrium we observe will also be symmetric. However, we see that the (lack of) balance in privacy levels is very dependent on topology. Some symmetric graphs like the complete graph and
cycle graph appears to always have a balanced, symmetric equilibrium. Star graphs have very imbalanced equilibria. This is unsurprising since the central node can take advantage of his position in the network and freeride off the information reveals by his neighbors. Bipartite graphs also exhibit specialized equilibria, even when they are symmetric (e.g., complete bipartite graphs). In the Nash equilibrium, nodes in one partition maintain very high privacy levels and free-ride off the nodes in the other partition, who have low privacy. This equilibrium is non-unique since a permutation of the nodes results in another Nash equilibrium.

We also examined the dependence of the equilibria behavior on $k$, a parameter for privacy cost. In figure 3, we look at the Nash Equilibria for varying integral values of $k$. Empirically, we see that for larger $k$, even in cases where there was previously an imbalanced equilibria (such as the bipartite case), the equilibrium that arises is a symmetric equilibrium. Note that the presence of a symmetric equilibrium in the figure does not necessarily indicate uniqueness of the Nash equilibrium. It is possible that the balanced equilibrium is unstable i.e., a small change in a user’s response from the equilibrium results in a new equilibrium.

4. WHEN DOES POLARIZATION OCCUR?

We can see in figures 3 and 2 that there is clearly a relation of the topology of the graph to the level of balance in privacy levels adopted in a network. We turn to the rich literature of the topology of the graph to the level of balance in privacy. This equilibrium is non-unique since a permutation of the nodes results in another Nash equilibrium.

We observe that $\phi'(\lambda_{-i}) \in [-\frac{2}{k+1}, 0]$. Thus, a sufficient condition for a unique Nash equilibrium is

$$\frac{1}{\mu_{\text{min}}} \leq -\frac{2}{k+1}. \quad (2)$$

We have shown these results numerically in figure 4, where we compare the values of $\phi'(x)$ to that of $\mu_{\text{min}}$ for several common graphs for the case of $k = 2$. In the case of a complete graph, since $\mu_{\text{min}} = -1$, we see that $\phi'(x)$ is always within the limits of network normality ($[-1, 0]$) (replicating the results in [8]).

**Corollary 5. ([8]) For a complete graph, there always exists a unique Nash equilibrium.**

However, we see that the story is more complex in other graphs. Complete bipartite graphs represent the extreme case since they have the smallest minimum eigenvalue of different graph types. We see that the bounds for network normality in the bipartite case are much tighter, showing that depending on the parameters, we might see a unique equilibrium but in many cases, there will be multiple equilibria.

**Proof.** As given in equation 1, the best response of agent $i$ to the privacy of her neighbors, $\lambda_{-i}$ is given as the solution to:

$$\lambda_{-i} \frac{d}{d\lambda_i} (\lambda_i + \lambda_{-i}) = \frac{1}{\sqrt{ck}}.$$  

The network normality condition is expressed as a derivative of the best response function. Implicitly differentiating the above equation w.r.t. $\lambda_i$ on both sides,

$$\frac{d}{d\lambda_{-i}} (\lambda^{k-1}_i (\lambda_i + \lambda_{-i})) = 0.$$  

Simplifying

$$\phi' (\lambda_{-i}) = \frac{d\lambda_i}{d\lambda_{-i}} = \frac{-2\lambda_i}{(k+1)\lambda_i + (k-1)\lambda_{-i}}.$$  

We observe that $\phi'(\lambda_{-i}) \in [-\frac{2}{k+1}, 0]$. Thus, a sufficient condition for a unique Nash equilibrium is

$$\frac{1}{\mu_{\text{min}}} \leq -\frac{2}{k+1}.$$  

$\square$

**THEOREM 4.** Let $\mu_{\text{min}}$ be the minimum eigenvalue of the adjacency matrix of the network $G(V,E)$ and let $k$ be the privacy cost parameter of the system. A unique Nash Equilibrium exists if $\mu_{\text{min}} \leq -\frac{2}{k+1}$.

**PROOF.** Let $\phi(x)$ be the best response function and $\mu_{\text{min}}$ be the minimum eigenvalue of the adjacency matrix of the graph. (Note, this is equivalent to $1 - \frac{1}{\mu_{\text{min}}} < \gamma'(x) < 1$ where $\gamma(x)$ is the engel curve for consumption).

$\square$
Figure 4: Derivative of best response function for various $c$, $k = 2$. Also shown are the minimum eigenvalues for a few specific graphs.

Remark 6. For cycle graphs and complete bipartite graphs, when there are quadratic privacy costs, i.e., $k = 2$, the network normality condition fails (an example of a non-unique equilibrium is seen in figure 2). This is because $\phi'(\lambda_{-i}) = \frac{-2\lambda}{3\lambda_{i} + \lambda_{-i}} \in [-\frac{2}{3}, 0]$. In an even cycle graph, $\mu_{\text{min}} = -2$. Thus $\frac{1}{\mu_{\text{min}}} \geq \frac{3}{2}$. Similarly, for a complete bipartite graph, $\mu_{\text{min}} = -\frac{n}{2}$. Even for very small $n$, $\frac{n}{2} > \frac{2}{3}$.

5. CONCLUSION

In many situations, including social networking services, privacy choices made by individuals affect others unequally. When it is the case, as the simple example of the local wage poll suggests, a rich behavior of steady state solutions emerge. An individual ability to remain private and enjoy a service radically differ from your comrades even when those are ex-ante identical.

These results motivate a much richer analysis of the interplay of networks and privacy. First, we ignored so far that privacy is not entirely a private good, as information disclosed by your friend may affect you. Similarly, utility of information is way more complex in general than a crude linear function of precision. Second, much more in depth analysis of the equilibrium, its stability, and the effect of topology on a users privacy choice can be done using similar tools. Third, one could design network-informed incentive inside the service to keep estimation relevant with a fair and collectively small privacy cost. We hope to encourage more work on these issues in the near future.

6. REFERENCES