

MEMORANDUM

To: Decision Maker about Privacy

From: MCM 2018 Team

Subject: Private Information: The Emergence of a New Asset

Date: Monday, February 12, 2018

1 Introduction

In the era of "anywhere, anytime", people now produce more data than ever before. The variety and volume of digital records that can be created, processed and analyzed will continue to increase dramatically. By 2020, International Data Corporation (IDC) estimates that the global amount of digital records will increase more than 40-fold.

The problem is to quantify the cost of privacy. That is, to establish a metric to evaluate the monetary value of keeping PI protected and the fees it would cost for others to possess or utilize PI. We consider private information (PI) as record of "everything a person makes and does". To make the problem clearer, several concepts need to be explained.

Domain of Private Information. An initial list of types of private information includes: Digital identity (e.g., names, addresses, phone numbers, demographic information, social network profile information, etc.); Relationships to other people and organization (social media, contact list and profiles); Communication data and logs (emails, SMS, phone calls, IM and social network posts); Media produced, consumed and shared (in-text, audio, photo, video and other forms of media); Financial data (financial transactions, accounts, credit scores, physical assets and virtual goods); Health data (health/medical records, medical history, medical device logs, prescriptions and health insurance coverage); Institutional data (government, academic and employment data).

Subgroup of Individuals. E.g. citizenship, professional profiles, age, education level, occupation, etc.

Risks. The risks involve loss of safety, money, valuable items, intellectual property (IP), the person's electronic identity, professional embarrassment, loss of a position or job, social loss (friendships), social stigmatization, or marginalization.

2 Solutions and Conclusions

Private information will continue to increase dramatically in both quality and diversity, and has the potential to unlock significant economic and societal value. To some extent, Private Information (PI) is similar to personal property (PP) and intellectual

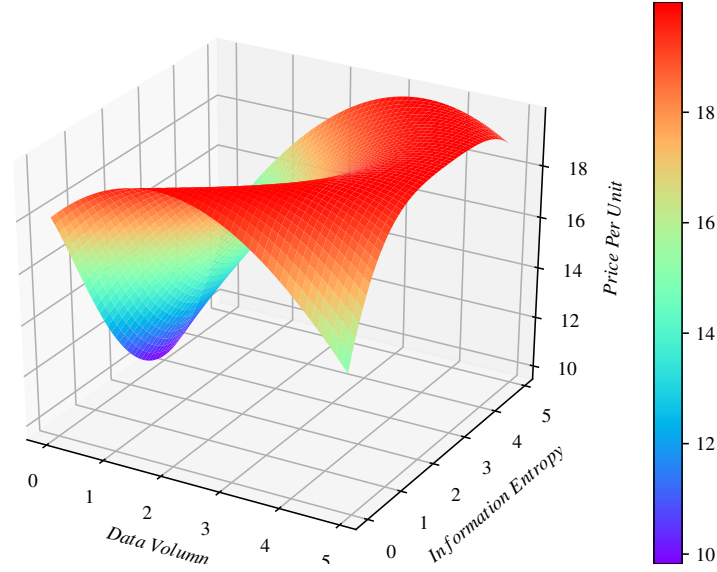


Figure 1: Demand Surface: the influence of data volume and information entropy

property (IP). However, there are also discrepancies among them. PI differs from PP and IP in that it can be sold or given to others who then have the right to use it without ownership, and it needs to be regulated by government. These information and privacy issues should be protected not only by the individuals but also by the agencies. Based on our model, the private data should not be trackable by the government for national security concerns.

Building a harmonious ecosystem around personal data will require significant commitment from all stakeholders. Our model proposes four critical solutions to deal with the problem:

- An expanded role for government, such that governments can use their purchasing power to help shape commercially available products and solutions that the private sector can then leverage;
- Mechanisms for enhancing trust among all parts in private information transaction;
- Integrate principles surrounding and user trust and data protection into the development of new services and platforms;
- Policy makers and agencies should launch an international dialog, which should encompass governments, international bodies such as the World Trade Organization, end user privacy rights groups and representation from the private sector. It should include not only US and European Union members, but interested parties from the Asia-Pacific region and emerging countries;