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 analysed will continue to increase dramatically. By 2020, IDC estimates that the global amount of digital records will increase more than 40-fold.

2 Problem Set Up

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 have or use PI. In this paper, we think of private information (PI) as record of "everything a person makes and does online and in the world." 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 and the like);
- Relationships to other people and organization (social media, contact list and profiles);
- Communications 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 (governmental, academic and employer 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.

3 Solutions & 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 extend, Private Information (PI) is similar to private personal property (PP) and intellectual property (IP). However, there is also discrepancies among them. PI is different from PP and IP in that it can be sold or given to others who then have the right to use but no ownership. The government should regulate this information. 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.

Potential gains from keeping data private include a greater level of security, especially for larger businesses. Potential lost from keeping data private include slowing down the pace of technological development. Notably, currently the development of *Artificial Intelligence* can not make such a big achievement without big data, e.g. ImageNet. Also, public sectors can trace the spread of disease in order to prevent further outbreak with shared private information, which is a welfare for most people. Commercial agencies can provide personalized service for different groups.

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;
- In the United States: Agencies should closely watch developments of the National Stategy for Trusted Identities in Cyberspace program and the privacy bill. Agencies need to be in constant dialog with the US Department of Commerce, the Federal Trade Commission and other bodies to help shape future legislation and policies; In the European Union: Agencies should collaborate with the European Commission in its move to revise the EU privacy directive. In other regions that differ from the US or the EU in cultural or social norms, very different paths in adopting policy frameworks will be required. One initial step in making progress could be to seek ways to harmonize fragmented national privacy policies.