Economics of Personal Data Management: Fair Personal Information Trades

A. Tasidou P.S. Efraimidis V. Katos

Department of Electrical and Computer Engineering,
Democritus University of Thrace,
Vas. Sophias 12, 67100 Xanthi, Greece
atasidou,pefraimi,vkatos@ee.duth.gr

Abstract. Individuals today have no control over the way their personal information is being used even though they are the ones to suffer the consequences of any unwanted uses of their information. We propose addressing this externality through the creation of a market for personal information, where licenses to access individuals' personal information will be voluntarily traded. Through this market, satisfactory compensation to the information owner is provided, whilst personal information remains under the owner's control. Using cryptographic tools and micropayments we propose and develop a prototype for personal information trades where the above principles are implemented and tested.

Keywords: Economics of Privacy, Information Markets, Privacy Enhancing Technologies

1 Introduction

The protection of personal privacy and the negative externalities that arise from the exploitation of personal information have become growing concerns for Internet users, as pointed out in [2] and [13]. Individuals provide their personal information to companies during online transactions. Such information lies at the company's disposal and can be used either for secondary uses inside a company, or even by making this information available to third parties, violating data protection-relevant policies [4]. Incidents of (un)intentional data loss are an almost daily occurence [9]. This situation can bring great profits to the parties who exploit the information and significant costs to the information owners, both financial and security related.

On the other hand, by processing personal information important benefits are brought to the marketplace for both companies and customers. Therefore, a fair, effective and legitimate way to acquire individuals' personal information for processing should exist. Besides, the aspiration of privacy protection technology is not to lock all personal information away from any possible access or use, but to allow access to personal information in a controlled manner. Moreover, it is possible that individuals would be willing to provide access to (some of) their

personal information in exchange for some profit, provided they could be assured of the safety of their information.

To this end, we consider the use of the Personal Information Market (PIM) concept, where access to personal information can be legitimately exchanged, providing at the same time mutual benefits to companies and individuals. In order for a PIM to be effective many challenges need to be addressed. First, it is important that personal information is exchanged in a way that misuse attempts are prevented or deterred. In this paper we address this challenge by using data licenses, which are based on cryptographic primitives. These licenses provide access to individuals' personal information under well specified conditions and therefore ensure that information owners do not lose control over their information.

We believe that an interesting analogy can be drawn between modern Internet users' privacy rights and developing countries producers' rights. Just like producers in such countries are vulnerable to work exploitation and suffer the consequences that arise from it, Internet users today suffer the exploitation of their personal information and the infringement of their privacy rights. Following this analogy, we propose an architecture named "*Fair* Personal Information *Trades*" (FPIT), that follows the principles of the Fair Trade movement, which offers better trading conditions to, and secures the rights of, marginalized producers and workers. [20]. Just like Fair Trade, FPIT can support fair trades of personal information between information owners and information consumers, while protecting their information owners' privacy.

In our view, the necessary technology exists today for better personal information management to be realized. The ideas and principles have been developed earlier and now the enabling technologies are present, both in information science and telecommunications, for them to be put into practice. In order for this to happen, there is a need for public demand for privacy protection which will in turn motivate companies to change today's situation. Apart from that, the necessary tools that use the recent technological advancements to create better privacy preserving conditions for well meaning companies and individuals need to be developed.

Outline.

The rest of this paper is structured as follows: In the following section we present some interesting related work. In Section 2 the FPIT concepts, architecture and components are described. In Section 3 the FPIT prototype is presented along with snapshots of test-runs. Finally, in Section 4 the contribution of this work is discussed, along with some open problems and some possible extensions and applications of FPIT.

Related Work

One of the first proposed markets for personal information was Laudon's National Information Markets [17], where personal information can be traded through a National Information Exchange. There are two major differences between Laudon's NIM and FPIT. First, in this work we follow a distributed

approach, where no third parties are involved for the information exchange. Second, in FPIT the personal information itself is never sold. Temporary access to personal information is sold, by means of appropriate licenses. Information users have to acquire information from their owners each time they need to use them, paying a small fee every time. A decentralized approach for information markets is Information Crystals [3]. This model aims at creating large groups of personal information, to be used aggregated for data mining, while protecting the owner's privacy. An interesting work that implements the idea of Personal Information Market (PIM) is [10]. In that approach, only preference and behavioral information is for sale and therefore privacy protection is achieved by keeping Personal Identifiable Information (PII) undisclosed. PII is defined as any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. In our work, both PII and preference/behavioral information can be exchanged. We argue that companies should be able to acquire individuals' contact information, with their consent, for marketing purposes. We achieve privacy protection by using data licenses and the convention that no information is allowed to be stored at the company's side. Another important differentiator is that our platform does not rely on the existence of trusted third parties for transferring personal information. Contemporary privacy enhancing technologies are presented in [9]. An interesting analysis on the economic aspects of personal privacy and how market mechanisms might solve privacy problems is presented in [19]. The economics of privacy are also discussed in [5, 14, 16, 15, 12]. An insightful analysis of the different approaches to personal information protection, including market-based approaches is presented in [11]. In that work the conclusion is drawn that it is very difficult to protect from unauthorized information copying and distribution. This is especially important for personal information, because there is no way of preventing a person allowed to see the information once, from writing it down on a piece of paper. This problem could be addressed by requiring information users to exhibit licenses from the information owners, entitling them to use this piece of information for this particular purpose. The benefits from the use of data licenses are discussed in [6].

2 Fair Personal Information Trades

In the following sections we provide a description of the FPIT concepts and its proposed architecture.

2.1 Concepts and architecture

The basic principle of FPIT is that the control of personal information should be maintained by its owner. Therefore, companies are not allowed to store individuals' personal information and use it without their consent. The main players in FPIT are the following:

- *Individuals* who voluntarily participate in FPIT, selling access to their personal information.

– *Companies* interested in collecting and processing personal information.

These players are represented in the FPIT architecture by the *entity* component. Both individuals and companies can be called *FPIT-users*, or just *users*.

The resource that is traded in FPIT is the personal information of individuals. This renders the task of storing, managing and retrieving personal data a very critical operation in FPIT.

2.2 Personal Data Management in FPIT

In order for FPIT to work efficiently, it must contain a privacy enhanced subsystem for the storage of the individuals' personal data. We call this subsystem the "Personal Data Management System" (PDMS). Due to the nature of FPIT, the management of personal data has to meet the following requirements:

– Personal data can only be stored at the owner's side.
– Personal data must always be accessible for licensed use.
– Information security must be ensured and information leaks should be prevented.

A system that satisfies the above requirements for the management of personal information is the Polis platform described in [7]. In Polis, for every individual there is a personal agent, which is constantly accessible over the Internet. The agent contains the personal information, the policies and the contracts of the individual. Each company also has its own agent, which contacts individuals' agents in order to retrieve (some of) their personal information. The functionality and services of the agents in Polis can be extended by implementing appropriate (cryptographic) protocols. We use this feature in the implementation of the FPIT prototype.

2.3 FPIT-users

Each FPIT-individual entity is characterized by its personal information and its policies. This architecture can be expanded to contain more sophisticated components, like a transaction logging service or a negotiation mechanism.

In order for FPIT to work efficiently, its agents need to have reliable Internet connectivity. This requirement is straightforward for companies. As far as individuals are concerned, constant connectivity is quite common today and is soon expected to become a given. Nevertheless, the protocol for personal information exchange described below could be implemented in such a way, that even if the agent of an information provider loses connectivity, there will be no monetary loss for the companies this user interacted with.

Personal Information Representation

Personal Information traded in FPIT can be Personal Identifiable Information (PII), like the name, phone number, address, birth date etc, as well as preference and behavioral information of a person. However, as this is work in

progress, we decided to first examine the market for trading PII. It is straightforward, though, to expand FPIT to deal with preference and behavioral information as well.

Personal Information can be represented in an XML schema like the one shown in figure 1. This representation is simple and efficient enough to suit the needs of FPIT. Personal information is organized hierarchically in a number of categories, each of which can contain appropriate subcategories. This scheme can be expanded according to the implementation and usage needs of FPIT.

```
<?xml version="1.0" encoding="utf-8" ?>
- <User Description="Personal Data">
  - <Name Description="User's Name">
      <Given Description="Given Name">John</Given>
      <Family Description="Family Name">Doe</Family>
    </Name>
  - <Home-Info Description="User's Home Contact Information">
    - <Postal Description="Home mailing address">
        <Name Description="Name on mailing address">John Doe</Name>
        <Street Description="Home street address">FPIT Street 10</Street>
        <City Description="City">FPIT City</City>
        <StateProv Description="State or Province">FPITia</StateProv>
        <PostalCode Description="Postal Code">11111</PostalCode>
        <Organization Description="Organization Name">FPIT</Organization>
        <Country Description="Country Name">FairInformationTradeLand</Country>
      </Postal>
      <Telecom>...</Telecom>
    </Home-Info>
  </User>
```

Fig. 1. Personal Information in FPIT

Policies and Licenses

Policies are integral components of FPIT trades. Agent policies define whether the agent will accept or reject a transaction request. A policy, represented in an XML schema, contains the following fields:

- *Principals*: The FPIT-entities.
- *Info-item*: Every distinct item of an information provider's personal information.
- *Purposes*: The set of purposes that entitle principals to retrieve data. Some indicative purposes are promotion and statistics. Further additions could be made according to specific transaction needs.
- *Usage restrictions*: Additional restrictions may exist that limit access rights to a specific number of accesses or a specific time interval, or both.
- *Charge*: Value and unit of payment and conditions for charging.

Another important component/concept of this architecture is the license. A license is used to set the rules under which a company is entitled to have access to an individual's personal information. Licenses play a key role in this work, since they are the mechanism that controls personal information use and distribution.

The architecture overview of FPIT is presented in Figure 2.

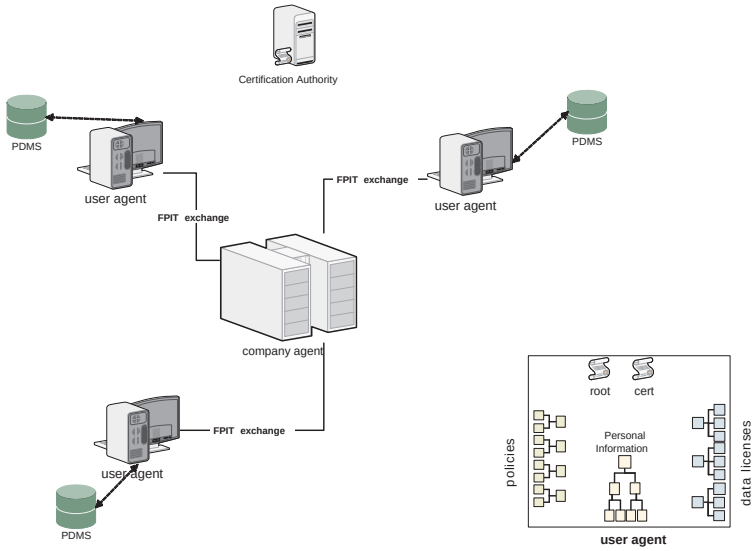

Fig. 2. The FPIT architecture overview

2.4 Payments in FPIT

The payment scheme within FPIT needs to be efficient enough to facilitate large numbers of small amount payments, without entailing substantial transaction costs. Therefore, we consider that micropayments as proposed in [18], suit the aforementioned needs.

The main actors in micropayment schemes are Brokers, Vendors and Users. A User becomes authorized to make micropayments by the Broker. A Vendor receives micropayments from authorized users and redeems them through the Broker. Relationships of Users and Vendors with the Broker are long term. The micropayment scheme we use in FPIT is Payword, presented in [18]. Payword is a credit-based scheme, based on chains of hash values (Paywords). Due to lack of space, the Payword protocol is not presented. For more information you can go to [18] or the long version of this paper [1]

2.5 Trading process in FPIT

Locating potential personal information providers can be achieved in several ways. The first and simplest solution is for companies to use their own clientèle database which would contain the agents' contact information of the clients that were interested in participating in personal information trades. Apart from that, other possibilities exist, like the creation of whitepages for participating individuals, or even participating agents' contact information exchanges between companies. In this work, we consider the act of locating the information provider

already accomplished and propose a protocol for the actual exchange of the personal information.

As far as pricing is concerned, i.e. the price per personal information item access, this is set to a fixed price of one Payword coin (usually representing the value of one cent). A pricing policy could be used in order to allow individuals to set different prices on their information items. For example, a person's phone number could be more expensive than their age. Prices could also vary depending on the time of day, or the season of the year. For example, acquiring one's phone number to call them during the evening or holidays could be more expensive. Pricing rules or even negotiation mechanisms could be introduced in FPIT as discussed in section 4.

Informal description of protocols

Once a company (information buyer) finds the contact information of an information provider's agent, the trading process can begin. The information trading process in FPIT consists of two phases: The Initial Agreement phase and the Purchase phase. These phases are described below:

During the Initial Agreement phase the following actions occur:

1. The information buyer contacts the information owner, sending a message about the kind(s) of personal information they are interested in, the period of time for which they are requesting access to the information and the price they are willing to pay for it. For example, an online shop might be interested in a person's e-mail for one year in order to send them promotional e-mails with offers and be willing to pay one coin for each e-mail.
2. The information owner's agent receives the request, checks whether it complies with its policies and responds accordingly.
3. If the request is accepted, the information buyer agent sends the commitment M, according to the Payword protocol.
4. The information owner verifies the buyer's certificate according to the Payword protocol.
5. If the verification is successful, a license is sent to the buyer, entitling them to the requested access to the owner's personal information.

After having established the initial agreement with the data owner, the data buyer can make several purchases, according to the agreed upon license. During a Purchase phase, the following actions take place:

1. The data buyer requests a specific item of personal information.
2. The owner's agent receives the request and verifies the accompanying license.
3. If the license is valid, an ACCEPT message is sent to the buyer's agent (verifying at the same time that the owner's agent is up).
4. The buyer sends the payment for the requested items according to the Payword protocol.
5. The owner's agent sends the requested information.

Using this protocol companies are protected from potential malicious information providers. The access to the personal information is not prepaid at Initial

Agreement phase and thus, information providers cannot receive their payment and disappear. Payment occurs each time an information item is requested. Therefore, the company can confirm that the information provider's agent is up before making any payments. The only way for an information provider to cheat is to receive the coin for the particular information item requested and then disappear. Even then, the gain for the information provider as well as the loss for the company will be minuscule. Besides, the company can always revoke the stolen Payword coin at the Broker.

3 The FPIT prototype

We implemented an FPIT prototype and performed proof-of-concept experiments. The main objective was to become acquainted with the practical difficulties intrinsic to a platform like FPIT. The prototype is implemented in *Java*. We use the *Bouncycastle* library for the cryptographic primitives. The management of the personal data is done with the Polis platform developed in [7]. The Payword micropayments used in the prototype are an adaptation of the Payword implementation in [8].

The development of the prototype proved to be straightforward.We used the following components for the experiment: An FPIT-shop, two FPIT-individuals and a Broker. The scenario of the experiment was that a shop named *shopfpit* buys and retrieves personal information from two FPIT-individuals, *alicefpit* and *bobfpit*. A snapshot of an agent used in FPIT is given in Figure 3.

In the FPIT prototype, we employ some security measures: the communication is performed over SSL sockets with both server and client authentication enabled. Contracts are digitally signed by both parties. However, at this stage we did not address malicious behavior or general fault tolerance issues. We are mainly interested in verifying the basic operations involved in the FPIT transactions and their efficiency.The main outcome of the experiments is that all the building blocks of the FPIT-platform work well. This confirms that the basic functionality of FPIT is attainable.

4 Discussion

We believe that Fair Personal Information Trades provides a straightforward proposal that could constitute a regulatory solution to the large scale privacy invasion that is currently perpetrated. In particular, FPIT sets well-defined, clear rules for the proper utilization of personal information, giving the ability to individuals to control and decide upon how information about themselves is used. Additionally, it provides a legitimate and fair, yet efficient enough, way for companies to acquire dynamic, up-to-date information, relevant to the purpose of their intended use. Hence, FPIT attempts to reduce information collecting companies' unrestrained personal information exploitation and motivates them to behave more responsibly. In general, FPIT puts the idea of compensating the

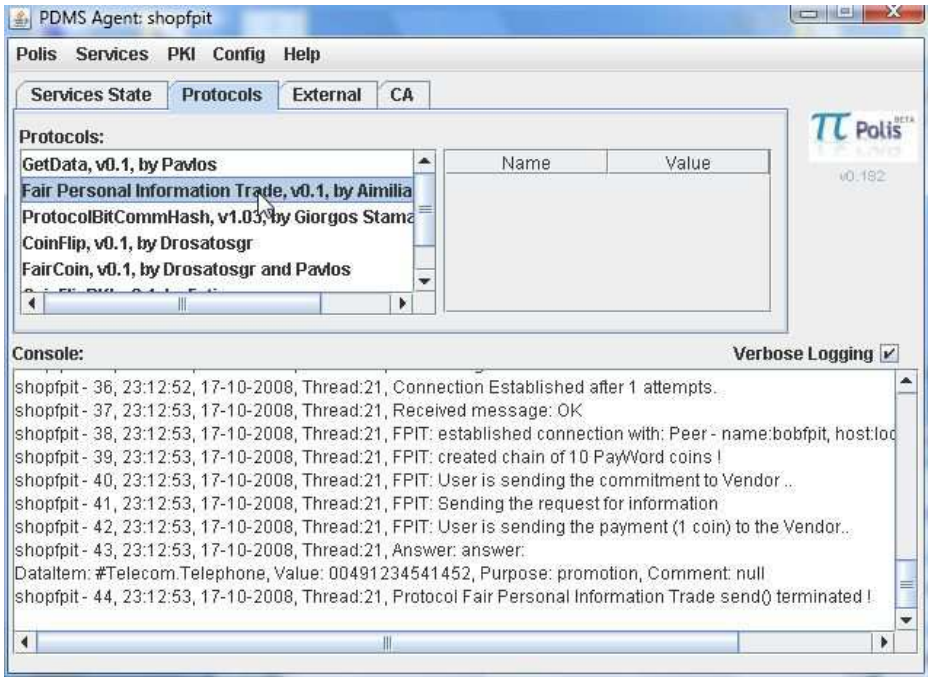

Fig. 3. FPIT agent snapshot

information owner into practice. It ensures that individuals who provide information are compensated for their service, while their personal information is being protected, at least as much as it is protected currently, but most possibly even more. Finally, it successfully combines the use of data licenses with the ideas of information markets and micropayments to propose a broader solution for trading personal information.

Open problems and future work

The underlying issues related to FPIT have a wide and transdisciplinar scope, as there are social, economical and technical challenges which need to be addressed. The following issues and problems have been identified, which mainly lie in the technical domain, as the main volume of our research is technically focused:

- Cryptography is sought to be the main technical enabler of the proposed infrastructure. As such, all (cryptographic) goals should be defined in order to evaluate the soundness of the underlying cryptographic protocols.
- Currently there is no distinguisher that can deterministically separate personal identifiable information from personal information. This leads to considering by default all personal information as identifiable, which forces the application of legislative protective controls to the whole data set, which in turn reduces efficiency of the proposed infrastructure.

– The proposed framework needs to revisit the business partnering model, as this constitutes well accepted business practices and excluding this from the framework is not a realistic assumption.

References

1. V. Katos A. Tasidou, P.S. Efraimidis. Economics of personal data management: Fair personal information trades. Technical Report LPDP-2009-01, Dept. Electr.& Comp. Eng., DUTH, Greece, 2009.
2. A. Acquisti. Privacy and security of personal information: Technological solutions and economic incentives. In J. Camp and R. Lewis, editors, *The Economics of Information Security*, pages 165–178. Kluwer, 2004.
3. Eytan Adar and Bernardo A. Huberman. A market for secrets. *First Monday*, 6:200–1, 2001.
4. R. Anderson. U.k. government loses personal data on 25 million citizens. *EDRI-gram*, Number 5.22, 21 November 2007.
5. R. Anderson and T. Moore. The economics of information security. *Science*, 314(5799).
6. Shi-Cho Cha and Yuh-Jzer Joung. From p3p to data licenses. In *Privacy Enhancing Technologies*, pages 205–222, 2003.
7. P. S. Efraimidis, G. Drosatos, F. Nalbadis, and A. Tasidou. Towards privacy in personal data management. In *PCI '08*, pages 3–7, 2008.
8. G. Georgakopoulos. Privacy enhancing technologies for personal data management. Master's thesis, Dept. Electr.& Comp. Eng., DUTH, Greece, October 2008.
9. Ian Goldberg. Privacy-enancing technologies for the internet iii: Ten years later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, editors, *Chapter 1 of Digital Privacy: Theory, Technologies, and Practices*. December 2007.
10. Ram Gopal, Robert Garfinkel, Manuel Nunez, and Daniel Rice. Electronic markets for private information: Economic and security considerations. In *HICSS '06: Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, Washington, DC, USA, 2006. IEEE Computer Society.
11. Rachel Greenstadt and Michael D. Smith. Protecting personal information: Obstacles and directions. In *WEIS '05*, 2005.
12. S. Gritzalis. Enhancing web privacy and anonymity in the digital era. *Information Management and Computer Security*, 12(3):255–287, 2004.
13. Bernardo A. Huberman, Eytan Adar, and Leslie R. Fine. Valuating privacy. *IEEE Security and Privacy*, 3(5):22–25, September 2005.
14. V. Katos and A. Patel. A partial equilibrium view on security and privacy. *Information Management & Computer Security*, 16:74–83, 2008.
15. S.K. Katsikas, J. Lopez, and G. Pernul. Trust, privacy and security in e-business: Requirements and solutions. In *PCI '05*, pages 548–558, 2005.
16. J. Kleinberg, C. Papadimitriou, and P. Raghavan. On the value of private information. *TARK: Theoretical Aspects of Reasoning about Knowledge*, 8, 2001.
17. K.C. Laudon. Markets and privacy. *Commun. ACM*, 39(9):92–104, 1996.
18. Ronald L. Rivest and Adi Shamir. Payword and micromint: two simple micropayment schemes. In *CryptoBytes*, volume 2, pages 69–87, 1996.
19. Hal Varian. Economic aspects of personal privacy. U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age, 1996.
20. Wikipedia. Fair trade. http://en.wikipedia.org/wiki/Fair_trade.