Increasing Trust Towards eCommerce
Privacy Enhancing Technologies Against Price Discrimination

Christos Makris[1], Konstantinos Patikas[1] and Yannis C. Stamatiou[2,3]

[1]*Dept. of Computer Engineering and Informatics, University of Patras, Rio, Patras, 26504, Greece*

[2]*Dept. of Business Administration, University of Patras, Rio, Patras, 26504, Greece*

[3]*Computer Technology Institute & Press – "Diophantus", N. Kazantzaki, University of Patras, Rio, Patras, 26504, Greece*

Keywords: Price Discrimination, Privacy Enhancing Technologies, Privacy ABCs, eCommerce, Personally Identifiable Information (PII).

Abstract: Price discrimination is a recently introduced practice in the domain of eCommerce. It is manifested by the appearance of different prices when the same product is browsed by different prospective buyers, based on their profiles. Thus, for instance, the price of an item may increase at the instance it is browsed by a user coming from a rich neighbourhood or has performed a series of purchases of expensive objects in the past. Price discrimination can lead to decrease of profits and loss of clientele, in the long run, as well as decrease of people's trust towards eCommerce. In this paper, we propose the deployment of Privacy Enhancing Technologies in order to handle users' personal information. These technologies empower users to have command over their own privacy by allowing them to reveal only what is absolutely necessary (minimal disclosure principle), or what they agree to reveal, in order to use a service avoiding any Personally Identifiable Information (PII). Thus, eCommerce services that employ such technologies for handling their clients' personal data can attract more loyal clients, increase their popularity while, at the same time, suffer from minimal client data and company image loss in case of a massive customer data theft attacks.

1 INTRODUCTION

Price discrimination, in the context of *privacy*, refers to the display of different prices (usually higher) for the same product to different users depending on their profile elements such as, for example, area of residence as well as purchasing behaviour and history.

Price discrimination is neither a new term nor describes, necessarily, a negative phenomenon in general. Its usual content in economy is that the price of a single item may change in three distinct ways or price discrimination degrees: 1) [First Degree] Charging different price for every item consumed, 2) [Second Degree] Charging different prices for different quantities, and 3) [Third Degree] Charging different prices to different consumers for the same item. The third degree price discrimination is the most usual one and it is this type to which we refer to in this paper.

Price discrimination is a complex phenomenon with multiple facets and plays a central role in shaping prices in economy and enterprise competition environments (Armstrong, 2006). However, in the context of our paper, we will study price discrimination in connection to *user privacy*, why it is not beneficial to commercial organizations and how it can be overcome by suitable privacy enhancing mechanisms.

Price discrimination, although it appears as something beneficial the for eCommerce vendors since it may lead to profit increase, it nevertheless poses a severe danger for the future of eCommerce due to the decrease of people's trust. Beyond the moral issue of violating the right of users to be offered the correct price, price discrimination hampers the widespread acceptance of eCommerce services because of fear of users that they can be the victims of such discrimination.

Work performed in the context of price discrimination within the eCommerce domain, which is related to users' privacy, has been carried out with respect, mainly, to identify it rather than prevent it (see Mikians *et al.* 2012 and Mikians *et al.* 2013). Since price discrimination is, essentially, based on gathering information about users, our view is that by

Makris, C., Patikas, K. and Stamatiou, Y.
Increasing Trust Towards eCommerce: - Privacy Enhancing Technologies Against Price Discrimination.
In *Proceedings of the 12th International Conference on Web Information Systems and Technologies (WEBIST 2016) - Volume 1*, pages 25-31
ISBN: 978-989-758-186-1

deploying technologies that protect users' privacy towards eCommerce sites can eliminate or, at least, limit the price discrimination phenomenon. These technologies, termed *Privacy Enhancing Technologies*, or PETs for short (see, e.g., Huberman, *et al.* 1999), give the power to users to reveal about themselves only what is absolutely necessary in order to use a service avoiding, thus, to reveal any *Personally Identifiable Information* (PII) (Narayanan, *et al.* 2010). In other words, contrary to customary user authentication methods such as the X509 certificates, which reveal all identity information towards a service, PETs allow users to reveal only a subset of their identity elements. Thus, for instance, they may choose not to reveal an element which they suspect or know that can subject them to price discrimination, such as their job or place of residence. Moreover, PETs allow users to present themselves with unlinkable, but certified, pseudonyms which are unlinkable and, thus, avoid profiling which is a powerful means for imposing price discrimination.

Our position, as we explain in this paper for the first time, to the best of our knowledge, is that PETs can boost trust towards eCommerce services in various ways. It may appear, from a superficial consideration, that eCommerce players would be reluctant to adopt PETs because they will prevent them from imposing price discrimination on their clients. However, we believe that this reluctance can be easily overcome since PETs can bring to eCommerce players the following advantages:

1. Establishment of trust and confidence of users in eCommerce, since they will know that their behaviour is neither monitored nor profiled and, thus, price discrimination is not possible.
2. Increased profits precisely because of the increased trust of users towards eCommerce services that deploy PETs. In other words users, based on the functionality of PETs, will be convinced that no price discrimination can take place and will tend to make more purchases.
3. Creation of a trust environment among sellers and buyers in the eCommerce ecosystem, which is expected to develop, further, eCommerce and increase its wider acceptance.

Based on the above, in this paper we present our approach on how PETs can be deployed towards the reduction of price discrimination using a recently released PET technology called *Privacy-ABCs*. Privacy-ABCs was the outcome of the research project ABC4Trust (for a summary see Sabouri, *at al.* 2012 and for all the details of the project see the ABC4Trust project book Rannenberg, *et al.* 2015).

2 PRIVACY-ABCs

Many electronic applications and services require authentication of participants in order to verify their eligibility to use them. Most authentication methods however, such as password based on X.509 based, have the negative consequence that the service actually knows who the user is since all the elements of the user's identity are revealed. If we exclude critical applications, such as eBanking for instance, in which full user authentication is mandatory, in most other online commercial applications it is not necessary for users to reveal their full identity or some of their identity elements. If they do, this leads to privacy problems, such as profiling, linking of online activities to a user, and history of purchases which in turn gives rise, by some eCommerce sites, to the phenomenon of price discrimination, based on what is known (to the sites) about the users (see Acquisti and Varian 2005).

The main Privacy Enhancing Technologies (PETs) available until the completion of the ABC4Trust project in February 2015 were IBM's Idemix (Camenisch and Lysyanskaya, 2001, Camenisch, and Lysyanskaya, 2004, and Camenisch and Groß 2012) and Microsoft's U-prove (Brands, 2000, and Brands, *et al.* 2007). The ABC4Trust project unified, transparently, these two technologies, adding more features along the way, and developed a new technology called Privacy-ABCs which supports, in an interoperable way, both the two pre-existing technologies.

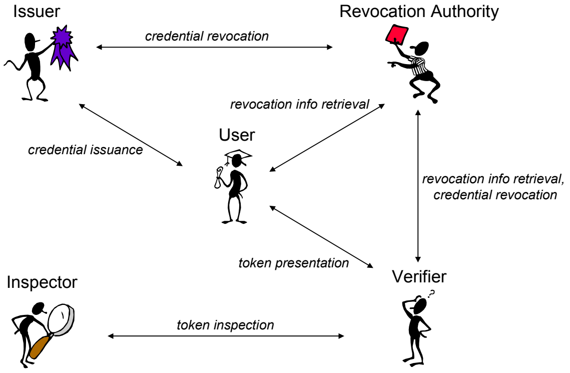


Figure 1: Entities and interactions diagram.

This section provides a brief description of the Privacy-ABCs elements and functionalities which we will exploit in order to guard users against price discrimination. Figure 1 gives an overview of the different Privacy-ABCs entities and their interactions (see Sabouri, *et al.* 2012).

We start our description of the basic privacy architecture entities by the Issuer. The Issuer constructs and provides credentials (e.g. on a smart card) containing identity attributes to the User. Upon request by the User, the Issuer generates the credentials by executing a credentials issuance protocol and, then, provides them to the User. The information that is contained in the credentials comes from either the User herself or the Issuer, if the Issuer already has this information. The credentials are signed by the Issuer who, in this way, attests for their correctness. For example, an Issuer could be attesting attributes of the User to the university for the attribute of students status, to the bar association for the attribute of being an advocate, and to the trade register for a company's commercial status.

The User is the service user who obtains her credentials from the Issuer through th issuance protocol. These credentials enable her to provide proof of the required identity attributes towards a Verifier (e.g. an eCommerce site).

The Verifier receives a presentation token from the User which process that the User possesses certain identity attributes. The Verifier (e.g. an eCommerce site) provides some kind of service to the User for whom it requires to know certain identity elements which, in turn, requires the User to either reveal or, simply, prove possession of these elements.

The Inspector, which is an optional entity, reveals the identity or other encrypted attributes of a User, thereby lifting her anonymity, upon a legal request. Legality is judged against previously defined criteria (e.g. fraud, service misuse etc.), clearly stated to the users when they first obtain credentials from the Issuer. Due to privacy subtleties involved in the Inspector entity, an Inspector building block should not be, by default, a part of a Privacy-ABCs platform but it should be included only after thorough consideration and if it is absolutely necessary. The issue of the Inspector has attracted many discussions which are beyond the scope of this paper since they involve, mostly, legal issues and depends on the specific mandates of personal data protection legislation (please see Bieker, *et al.* 2015 for a thorough discussion on these issues).

The Revocation entity is responsible for revoking issued User credentials. If revoked, the credentials cannot be used for producing valid proofs about credentials (i.e. presentation tokens). The Revocation entity is, again, an optional component of a Privacy-ABCs system. Often, the entity offering the Revocation service is the same as that offering the Issuer service, since the Issuer can be assumed to have the most up-to-date and complete information about users.

In an actual deployment, some of the above entities may, actually, be implemented by the same entity or be split among many different entities. For example, an Issuer can, at the same time, have the role of Revocation Authority and/or Inspector, or an Issuer could later also be the Verifier of tokens derived from credentials that it issued itself.

In Figure 2 we can see the generic Privacy-ABCs architecture based on the entities/services described above. The focus in this description is on generality rather than attention to the peculiarities of a specific use case, one of which we are going to examine next in the context of price discrimination.

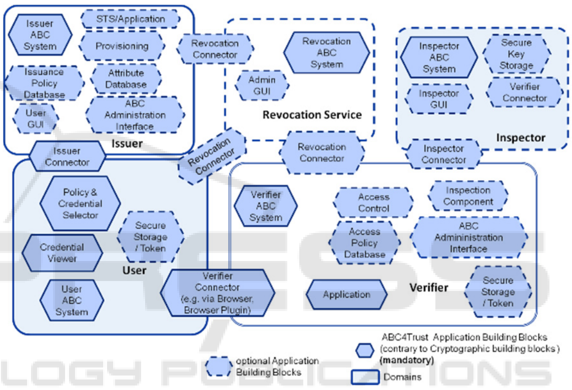


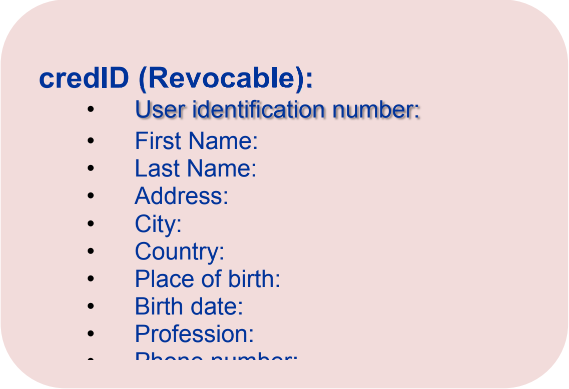
Figure 2: A generic Privacy-ABCs architecture.

3 PRIVACY-ABCs AGAINST PRICE DISCRIMINATION

In this section we explain how Privacy-ABCs can be exploited in order to protect eConmmerce site users from price discrimination. To this end, we describe the roles of the identities that we discussed in the previous section. All implementations can be based on the Privacy-ABCs reference implementation available at Github (please visit https://github.com/p2abcengine/p2abcengine).

Our first entity, the *Issuer*, can be a major eCommerce player that agrees to assume the responsibility of issuing credentials to the Users. The Issuer, alternatively, can be a governmental agency (e.g. Ministry of Commerce) that assumes this role in order to create an eCommerce environment without price discrimination for users. The Issuer is implemented by the modules in the Issuer block in

Figure 2. The credential issued to users includes basic information (attributes) about a user's identity and it looks like the following:



credID (Revocable):

- User identification number:
- First Name:
- Last Name:
- Address:
- City:
- Country:
- Place of birth:
- Birth date:
- Profession:
- Phone number:

We can see that this is the usual information found in a customary eIdentity card or certificate (e.g. X.509) plus, perhaps, some other information useful in an eCommerce environment such as, for instance, whether the user has a credit card or not (last attribute in the credential figure).

The major differences from the customary identification schemes lie in the following two features:

- The user is in power to reveal *only* the credential attributes that she desires to reveal (or agrees to reveal according to the eCommerce site policy).
- The user can prove a *property* about an attribute, without revealing it. For instance, the user can prove that her age is above 18 without revealing its exact value.

Verifiers, i.e. eCommerce sites, who wish to operate in an eCommerce environment against price discrimination, should develop their eCommerce platform based on the Privacy-ABCs reference implementation. The Verifier contains the modules shown in the Verifier block in Figure 2.

Users should install the modules shown in the User block in Figure 2 on the devices through which they visit eCommerce sites. The installation is very easy and convenient while it induces minimal computation overhead on the device (see Benenson, *et al.* 2013 and Benenson, *et al.* 2014 for more on the user satisfaction survey we conducted within the context of the ABC4Trust project).

We consider the Revocation and Inspector entities unnecessary for an eCommerce environment against price discrimination and, thus, we do not include a role for them.

4 AN EXPERIMENTAL ECOMMERCE SITE BASED ON PRIVACY-ABCs

The ABC4Trust project has made the Privacy-ABCs code and support modules available through the Github repository. They are freely offered for prospective developers of any application that requires privacy preserving authentication methods.

The application we present in this section was built, relatively easily, using the Githtub Privacy-ABCs modules. It is a prototype eCommerce application, named Grails, for selling online a variety of products. It is based on the Grails Hotel Reservation demo application offered by the ABC4Trust project in Github in order to demonstrate the easiness with which one can build a complete eCommerce application based on the modules available from the project.

The application uses the privacy features of Privacy-ABCs in order to enhance users' trust that they are not subjected to price discrimination while they are making their purchases. The additional feature the is not often found in usual eCommerce sites and which is based on the properties of Privacy-ABCs is that it allows *duty free shopping* to byers who can prove that they have a valid passport issues in another country. The passport owner simply proves the possession of the passport as well as the country of issuance, keeping all other personal information secret.

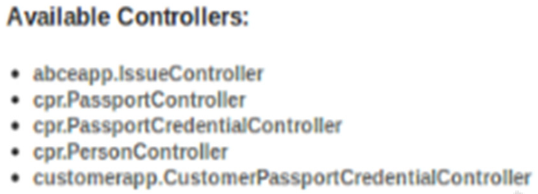
The system is composed of the following subsystems and modules:

- A Grails application carrying the webpage of the online vendor, acting as the *Verifier* of buyers' passport and credit card credentials. Throughout the verification process, the buyer's anonymity is preserved due to the properties of Privacy-ABCs.
- A Grails application with the webpage of a bank which issues credit card credentials to users, acting as an *Issuer*.
- A Grails application with the webpage of a governmental agency which issues passport credentials, acting as a second *Issuer*.
- A *Revocation* service for revoking credit card credentials due to credit card theft or expiration.
- A User service for managing the user's credentials, the communication with the user's smartcard which contains the credentials and performing the presentations of credentials.

- A user UI (User Interface) service, providing a GUI (Graphical User Interface) for the User service.

After booting the virtual machine containing all the eCommerce application modules described above (in a simulated eCommerce environment) one simply logs on with the password "abc4trust". All the necessary system services for for revocation authority, vendor verifier, passport issuer, credit card issuer, user service and UI service, are activated automatically.

We can see the available credential issuance controllers below as they appear on the user's screen:

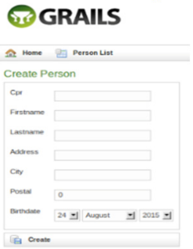


Available Controllers:

- abceapp.IssueController
- cpr.PassportController
- cpr.PassportCredentialController
- cpr.PersonController
- customerapp.CustomerPassportCredentialController

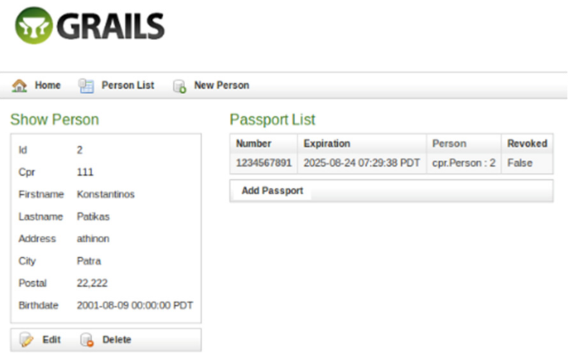
The objective of the application is to allow users to buy a product from an eCommerce site without subjecting them to price discrimination. The site does not require from users to show their names or other details such as country of origin or place of residence, which could, possibly, allow the eCommerce site to infer some information that could lead to price discrimination against the user. The users only have to prove that they possess a valid credit card and a passport showing the appropriate credentials, uncovering *only* the country of password issuance.

A user wishing to use the Privacy-ABCs features with this eCommerce site should start by obtaining a passport credential from the Issuer. The Issuer maintains a database of people eligible for a passport credential (possibly by contacting a governmental agency or authority). In order to be able to get a credential issued, a user has two options. Either you can use a preexisting credential, or you must create a new person, attach a passport to this person and finally attach a credential to the passport.



Create Person

Cpr
Firstname
Lastname
Address
City
Postal 0
Birthdate 24 August 2015



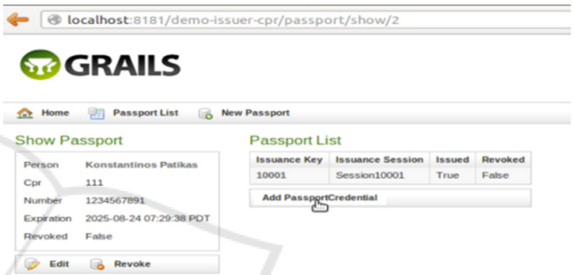
Show Person

Id	2
Cpr	111
Firstname	Konstantinos
Lastname	Patikas
Address	athinon
City	Patra
Postal	22,222
Birthdate	2001-08-09 00:00:00 PDT

Passport List

Number	Expiration	Person	Revoked
1234567891	2025-08-24 07:29:38 PDT	cpr.Person : 2	False

After creating a new user identity, we create a new passport and we attach it to the person. Furthermore, we have the option of creating a credential for the passport.



localhost:8181/demo-issuer-cpr/passport/show/2

Show Passport

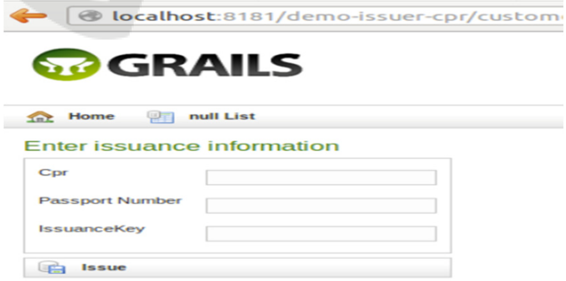
Person	Konstantinos Patikas
Cpr	111
Number	1234567891
Expiration	2025-08-24 07:29:38 PDT
Revoked	False

Passport List

Issuance Key	Issuance Session	Issued	Revoked
10001	Session10001	True	False

Finally, we will enable issuance of credentials for the newly created passport. As mentioned earlier, it is also possible to use a pre-existing credential. At this point, we should write down the values for cpr (ID number), passport number and issuance key, as they are the required values for issuance.

Now you are ready for the actual issuance. We can start the issuance by filling in the fields with the values from above and clicking "Issue".

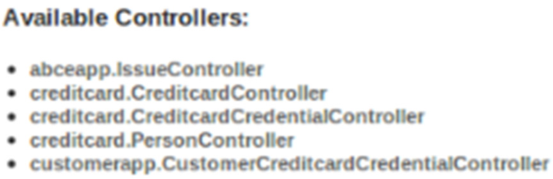


localhost:8181/demo-issuer-cpr/custom

Enter issuance information

Cpr
Passport Number
IssuanceKey

The process of issuing a credit card credential is similar to issuing a passport credential. We use the above controllers.



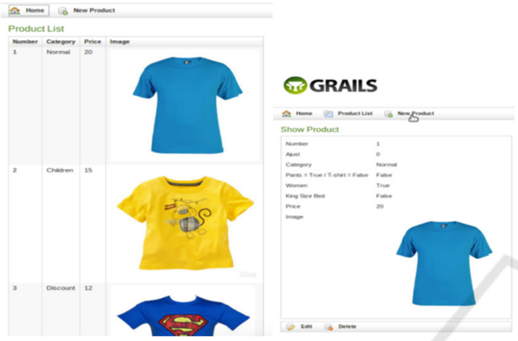
Available Controllers:

- abceapp.IssueController
- creditcard.CreditcardController
- creditcard.CreditcardCredentialController
- creditcard.PersonController
- customerapp.CustomerCreditcardCredentialController

As with the passport issuance, again it is possible to either create your own user identity or use a preexisting one if it exists. The process of creating a new user identity for the credit card credential is identical as the one described above for the passport.

Having obtained the password and credit card credentials, the user can then proceed to the eCommerce site to perform, anonymously and without being price discriminated, her purchases.

Also, the sample site we created allows the vendor to add products and edit their characteristics.



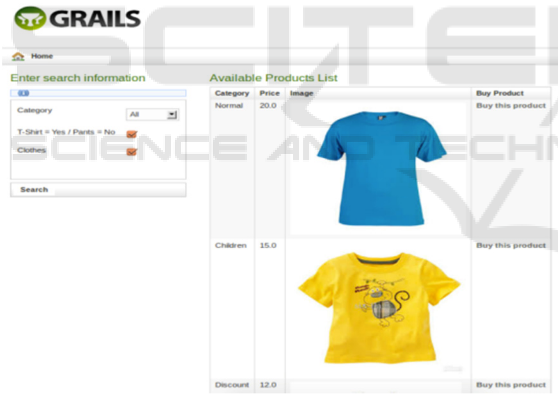
Product List

Number	Category	Price	Image
1	Normal	20	
2	Children	15	
3	Discount	12	

Show Product

Number	1
Ajust	0
Category	Normal
Pants = True / T-shirt = False	False
Women	True
King Size Bed	False
Price	20
Image	

The user is able to search using product search criteria in order to locate the desired product.



Enter search information

Category: All

T-Shirt = Yes / Pants = No ☑

Clothes ☑

Available Products List

Category	Price	Image	Buy Product
Normal	20.0		Buy this product
Children	15.0		Buy this product
Discount	12.0		Buy this product

Once the product is found, the user submits the purchase order by clicking on the “Submit” button. Then an Privacy-ABCs presentation token is send over to the vendor to certify that the user has a valid password and valid credit card credential.

The vendor site verifies the token and the webpage displays the “Verification was successful” message to the user, signifying acceptance of the order at the shown price. What is important is that throughout the purchase process, nothing is known about the user except that she has a valid passport and a valid credit card. After the process is complete with the shown product price, the user can enter a second interaction protocol with the vendor whereby she reveals her real identity in order to receive the goods.

5 CONCLUSIONS

Price discrimination is not a new phenomenon in commerce. Moreover, it does not necessarily have negative implications for the consumer or the seller. In recent years, however, price discrimination appears to cross the border of consumers' privacy and exploit personal information in order to adjust prices offered to consumers for maximizing profit.

In this paper we argued that a new Privacy Preserving Technology, Privacy ABCs, can be exploited towards creating an eCommerce ecosystem in which price discrimination is not possible due to the preservation of consumers' privacy, while they are still able to prove facts about themselves which are necessary in order to perform a purchase.

Our point of view is that price discrimination, although it appears beneficial to eCommerce sites, it destroys the trust relationship between sellers and buyers which can lead, in the long run, to financial losses due to loss of customers or, even worse, financial losses due to convictions because of leaks of personal data of the customers.

Of course, there are counterarguments to our point of view. The first one is that eCommerce players aim at building close relationship with their customers in order to serve them best. To this end, they need to know as much about them as possible in order to match their needs and, even, reward their loyalty. For instance, returning customers may be offered some special products or services best suited for them, based on their purchase history or other personal information that has been provided by them. The other counterargument is that most people bake online purchases from special applications downloaded to their mobile devices (either phones or tablets) which ask of the users to fully identify themselves in order to proceed to make purchases. Thus, there appears that giving personal information is either beneficial to the buyer (first counterargument) or even mandatory (second counterargument). With respect to the first argument, we should stress the fact that we are not against customer loyalty programs or benefits given to them based on their personal information and purchase history. It is the price discrimination in increasing prices based on such information which we attempt to reduce using PETs, at least for customers who perform purchases from a variety of eCommerce sites and are not much interested in rewards so as to provide personal information or allow tracking of their buying behaviour. With respect to the second argument, the dilemma of the buyer, when faced with the application's request to provide identifying information, is the following: "Should I proceed with the purchase, giving the requested personal information or to decline and leave the site?". We believe that our approach can offer a compromising solution for both the eCommerce site and the buyer: the eCommerce site can ask for information related to, e.g., the buyer's preferences, desires etc. or ask of the buyer to prove something about herself such as, for instance, that her age is at least 18. Such information may still be used by the site in order to provide tailored services to the user, without breaching the user's privacy with the risk of the buyer being subjected to price discrimination.

We believe that the "price or no price discrimination" question is not easy to settle. Our paper can at least be a starting point for further discussions. Technically, PETs can help reduce the price discrimination phenomenon and boost buyers' trust towards eCommerce vendors. Of course, it is also necessary to create a suitable policy framework in which it is clear what information is necessary for what types of services and convince all stakeholders to respect it (vendors and byers alike). The technology for protecting privacy is here but what remains is to assess its usefulness and applicability in the price discrimination phenomenon.

REFERENCES

Acquisti, A.,Varian, H.R., 2005. Conditioning Prices on Purchase History. *Marketing Science. Vol. 24, Issue 3.*

Armstrong, M. 2006. Recent Developments in the Economics of Price Discrimination. In *Proc. Advances in Economics and Econometrics: Theory and Applications, Ninth World Congress,* Cambridge University Press.

Benenson, Z., Krontiris, I., Liagkou, V., Rannenberg, K., Schopf, A., Schröder, D., Stamatiou, Y. C., 2013. Understanding and Using Anonymous Credentials. In *Proc. 9th Symposium on Usable Privacy and Security (SOUPS 2013).*

Benenson, Z., Girard, A., Krontiris, I., Liagkou, V. Rannenberg, K. Stamatiou, Y. C., 2014. User Acceptance of Privacy-ABCs: An Exploratory Study. In *Proc. of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust (2nd HCI International 2014), pp. 375-386,* Springer-Verlag.

Bieker, F., Hansen, M., Mikkelsen, G.L., Obersteller, H., 2015. *ABC4Trust Workshop on Core Features of Privacy-ABCs, Practical Use, and Legal Issues. Privacy and Identity Management for the Future Internet in the Age of Globalisation*, Volume 457 of the series *IFIP Advances in Information and Communication Technology*, pp. 253 – 266, Springer-Verlag.

Brands, S., 2000. *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. First Edition,. The MIT Press.

Brands, S., Demuynck, L., Decker, B. De., 2007. A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users. In *Proc. 12th Australasian Conference on Information Security and Privacy (ACISP 2007), pp. 400-415*, Springer-Verlag.

Camenisch, J., Lysyanskaya, A., 2001. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001), LNCS, pp. 93-118.* Springer-Verlag.

Camenisch, J., Lysyanskaya, A., 2004. Signature Schemes and Anonymous Credentials from Bilinear Maps. In *Proc. 24th International Conference on Cryptology (CRYPTO 2004), pp. 56-72,* Springer-Verlag.

Camenisch, J., Groß, T., 2012. Efficient attributes for anonymous credentials. *ACM Transactions on Information and System Security (TISSEC), Vol. 15, Issue 1, Article No. 4,* ACM Press.

Huberman, B. A., Franklin, M., Hogg, T. 1999. Enhancing privacy and trust in electronic communities. In *Proc. 1st ACM Conference on Electronic Commerce, pp. 78–86*, ACM Press.

Mikians, J., Gyarmati, L., Erramilli, V., Laoutaris, N. 2012. Detecting price and search discrimination on the internet. In *Proc. 11th ACM Workshop on Hot Topics in Networks, pp. 79 – 84*, ACM Press.

Mikians, J., Gyarmati, L., Erramilli, V., Laoutaris, N., 2013. Crowd-assisted Search for Price Discrimination in E-Commerce: First Results. In *Proc. 9th International Conference on merging Networking Experiments and Technologies (CoNEXT 2013)*. ACM Press.

Narayanan, A., Shmatikov, V., 2010. Myths and fallacies of "personally identifiable information". *Communications of the ACM*, 53 (6): 24, ACM Press.

Rannenberg. K., Camenisch, J., Sabouri, A, *eds.*, 2015. *Attribute-Based Credentials for Trust: Identity in the Information Society*. Springer-Verlag.

Sabouri, A., Krontiris, I., Rannenberg. K. (2012). Attribute-Based Credentials for Trust (ABC4Trust). In *Proc. 9th International Conference, on Trust, Privacy, and Security in Digital Business (TrustBus)*. Springer-Verlag.