Computer Ethics - Philosophical Enquiry (CEPE) Proceedings

Volume 2019 *CEPE 2019: Risk & Cybersecurity* Article 5

5-28-2019

Keeping Anonymity at the Consumer Behavior on the Internet: Proof of Sacrifice

Sachio Horie
Graduate School of Informatics Nagoya University

Keeping anonymity at the consumer behavior on the internet: Proof of sacrifice

Horie Sachio
Nagoya University

Abstract

The evolution of the Internet and AI technology has made it possible for the government and the businesses to keep track of their personal lives. GAFA continues to collect information unintended by the individuals. It is a threat that our privacy is violated in this way. In order to solute such problems, it is important to consider a mechanism that enables us to be peaceful lives while protecting privacy in the Internet society. This paper focuses on the consumption behavior on the Internet and addresses anonymity. We consider some network protocols that enable sustainable consensus by combining anonymity methods such as I2P and anonymity currency as anonymity protects our lives from the engineering , and its application and clarification. As a result, we could propose a new consensus protocol, Proof of Sacrifice.

Keywords: GAFA, consensus protocol, Channel Theory, anonymity

The evolution in computer science have led to the expansion of the Internet on a global scale. The benefits are immeasurable. For example, the information has become easily available, and cheap, high-quality products can now be purchased easily. However, changes in our lifestyle brought about by the Internet, mobile terminals and IoT are more than mere convenience improvements. For example, the evolution of image recognition technology leads to the analysis of images sent by third parties from smartphones. These technologies enable governments and large corporations to keep track of their personal lives. In fact, some IT companies represented by GAFA have already collected information at the user's intention. Security company UpGuard released the investigation report that it confirmed the data of Facebook in the state of release on Amazon. These data appear to have been acquired by a third party app from Facebook.

Some people may fall into pessimism and denial of science and technology in the face of such problems. But is the Internet society really incompatible with personal privacy? We think that we should focus on technologies for achieving anonymity on the Internet. The information engineers have proposed and developed various protocols that realize anonymity, including P2P networks. That's because they considered privacy protection important.

Of course, as Kevin Mitnick speaks, technology that does not expose itself to the Internet is in a range that can be done by individuals, but in this paper, as the scalability of technology transforms society, as a community, we considered the method to secure the anonymity.

In this paper, from the viewpoint of protecting privacy on the Internet, we try to

formalize the application of the existing anonymization network and how the anonymization network can be positioned as a sender and receiver of information, and consider a sustainable consensus protocol.

Anonymity and Privacy

When we act on the Internet, such as visited websites and visited web services, we are recorded our acts. These traces are primarily personal information, but are available to anyone beyond the time limits set by the principle of digital data integrity. If the data is explicitly deleted, it is still accessible through storage mechanisms such as "cached".

Governments and private companies constantly monitor the Web to collect and correlate information used to analyze user behavior. Monitoring is the most important activity of many the government in tracking political opponents and anti-social opponents. In addition, personal information as a trace left on the Web is extremely valuable to the service provider. When using freemium-type services such as Google and Facebook, we provide many personal information to the operator. The personal information is not limited to information such as name and age. For example, the operator can use information such as time zone or position information when using the service, action pattern by activation time, hobby preference by browsing data of the Web site, etc. They do the business by acquiring a large amount of information and delivering higher targeting ads.

According to a survey of the World Wireless Communications Agency (WARC), Google and Facebook have already accounted for about 25% of global Internet advertising in 2017. This means that they are able to deliver highly accurate ads, making them realize that they are collecting so much user information. Acquiring a large amount of personal information also means that the risk of information leakage is side by side. If the leaked personal information is used for something not intended by the individual, it can lead to a threat to our lives.

Since such a thing is actually happening, the demand for anonymity is increasing in recent years to cope with the large-scale spread of monitoring platforms deployed worldwide. Certainly, the concept of the anonymity may involve antisociality, as it includes the possibility that it leads to illegal activities. However, anonymity plays an important role in our political and social debates. We want to hide our "identity" as we may be concerned about political or economic, even threats to our lives.

So how do you anonymize? In the Internet, all terminals can hide IP addresses by using the anonymization service networks such as I2P and Tor. Implementation of the anonymization process is based on routing information. While transmitting data between two nodes in the network, it is impossible to know in the advance the route between the source and the destination, and each node of the network does not save the packet history without saving its history on the route.

In order to avoid surveillance, an encryption algorithm is used that makes it impossible to eavesdrop on the information and reconstruct the original message.

The important properties that realize anonymity are non-connectability and non-observability. In the situation where an act or a trace of an act is observed but it is not known who the actor is, it is considered that there is a possibility of non-connection of

the trace of the act or the act and non-observability of the actor. In anonymity, if it is accompanied by an illegal act provided by the degree of anonymity or an act that bothers another person, it must be recognized as a situation requiring a solution. It is sometimes requested as a mechanism to pursue legal responsibility, customs, moral accountability, etc.

Protecting the anonymity of the sender and receiver of information is to satisfy the following requirements.

a) Securing connection routes: Secure communication routes using techniques such as I2P and anonymous passage.

b) Concealment of communication content: The communication route is concealed using technology such as I2P and anonymous passage.

c) Encryption of transmission and reception addresses: The transmission source address and the recipient address are concealed using a one-time address or the like.

From the next section, I will explain I2P, an anonymous currency, which is one of the anonymization service networks related to our goal.

I2P and Anonymous Cryptocurrency

There are shouw below.
I2P: https://ieeexplore.ieee.org/document/7475027
Anonymous and secure Cryptocurrency:https://medium.com/piratechain/piratechain-anonymous-and-secure-crypto-currency-edf5625307c7

Example

Our goal is to propose how to protect privacy by applying these technologies. Alice and Bob are participants of the community for anonymity. We consider that Alice purchases an item to be purchased at Company P using anonymity. We do not consider the cost and incentive of the proposed system. The costs and incentives are discussed in the next chapter.

1) Alice accesses Company X via Bob using anonymous currency.
2-1) At this time, the billing information of Bob is used.
3-1) If the product is digitized, Bob should send information to Alice using I2P.
3-2) Next, if the product is not digitized, Company X delivers it to Bob.
3-2-1) Bob delivers it to Alice. At this time, Bob knows the physical address of Alice.
3-2-2) A part of anonymous currency held by Alice is converted to Bob's the cost of shipping cost and service cost (fee). Alice and Bob know the physical addresses of other participants including themselves.

Consensus protocol

The essence of this example is the question of whether it is possible to create a

consensus protocol with fault tolerance among unknown participants under certain "conditions" called "anonymity" (in fact, even if there is a condition) Under the condition that the total number n of nodes is not determined, it is said that no protocol satisfying the consensus exists: General Byzantine problem.

In addition, the consensus building described in this paper is premised on being formed by human interests in advance.

In this example, there are individuals who want to protect personal information, communication is made in a distributed system called community, and from the perspective of the community, individuals play their respective roles and behave as if they are selfish. However, because there is also the autonomy that individuals should have, such a community must maintain a structure that prevents participants from betraying it. To that end, incentives and costs are important.

It is very difficult to design an incentive structure that does not allow any anonymizing network participant to abuse its structure. In this paper, we solve the maintenance of the protocol by having one participant sacrifice anonymity, for example, actively participating in the purchase of other participants (= increase the fee). This is called Proof of Sacrifice. However, if the fee is too high, the client will be reduced, otherwise the number of agents who will purchase will be reduced. Therefore, only approximate solutions can be obtained.

From a game theory point of view, the cost of the anonymization network service, ie the negotiation cost (the cost required to reach an acceptable agreement for both parties in the transaction with other participants) If it increases, it will eventually outweigh the potential participants' perceived gains. That is because the anonymization network service must be fair and operate according to the rules defined for the software used.

Finally

In this paper, we considered the anonymization network. As a result, it was possible to clarify the flow of personal information between an individual and an institution by means of a method and channel theory that can realize anonymization specifically. In addition, although the cost and incentive structure must be solved for this kind of problem, this paper proposes the Proof of Sacrifice. However, formalization is a remaining issue. We would like to consider using channel theory(Appendix. A).

Finally, anonymized network services are more expensive than ordinary network services. The only reason to use anonymization network services in such situations is that anonymity allows the user to prevent monitoring and monitoring of activity on the Internet not only from businesses but also from government intervention. And future technology should protect basic human rights despite conflict with the spirit of law. However, the importance of anonymity on the Internet for both free speech and privacy is finally recognized, and there is no answer whether it will affect the Internet in the future.

References

谷卓史，“インターネットにおける匿名性はいかに正当化されるか?，”吉備国際大学政策マネジメント学部研究紀要，第3号，2007

折田明子:ネット上のCGM利用における匿名性の構造と設計可能性.情 報 社 会 学 会 誌Vol.4 No.1pp5-14 ,2009

Anonymous (Author is Scott, C.R.) “To reveal or not to reveal: A theoritical model of anonymous communication” Communication Theory,8 pp381-407,1998

Nunamaker, J.F. Jr. et al ”Information Technology for Negotiating Groups: Generating Options for Mutual Gain”.Management Science Vol.37 No.10 October 1991 pp1325-1346,1991

谷口展郎、千田浩司、塩野入理、金井敦:
分散アイデンティティエスクローにおける匿名性 / 仮名性 / 本人性の管理に関する考察. 電子情報通信学会技術報告 技術と社会・倫理研究会(SITE) 2005-53 pp.7-12,2006

Derlega, V.L. et al”Privacy and Self-disclosure in social relationships”,Journal of Social Issues, 33 pp102-115, 1977

中田響: 個人情報性の判断構造.
慶應義塾大学メディア・コミュニケーション研究所紀要 No.57, pp.145-161,2007

Pfitzmann, A. and Hansen, M. “Anonymity, Unlinkability,Undetectability, Unobservability, Pseudonymity, and Identity Management –A Consolidated Proposal for Terminology (Version v0.29 July 31, 2007)

伊地知晋一：CGMマーケティング : 消費者集合体を味方にする技術.
ソフトバンククリエイティブ.2006

折田明子,江木啓訓「リンク不能性および一覧性の観点による匿名性の分類」情報処理学会第37回電子化知的財産・社会基盤研究会, 2007

D. Howe and H. Nissenbaum (2017) "Engineering Privacy and Protest : a Case Study of AdNauseam," Proceedings of the Third International Workshop on Privacy Engineering San Jose, California, USA, 57-64.

Appendix A. Toward formalization by the channel theory

・ Informal explanation of channel theory

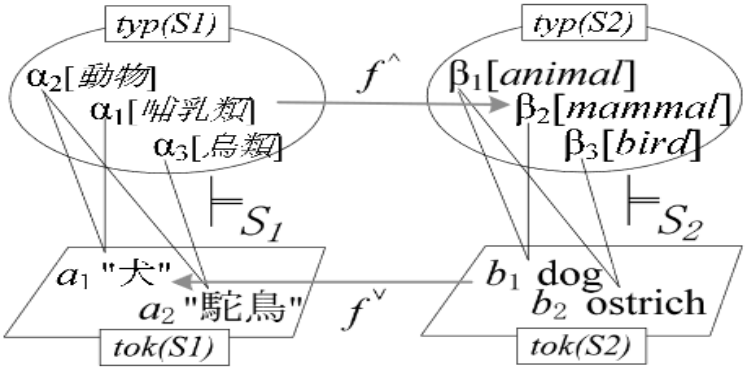

Fig.1 Classification

In the classification S1, “α2 [animal]”, “α1 [mammal]”, “α3 [birds]” are called type typ (S1), and “a1 dog”, “a2 bird” are called token tok (S1) .In the classification S2, “β1 [animal]”, “β2 [mammal]”, “β3 [bird]” are typ (S2), "b1 dog" and "b2 ostrich" are tok (S2). When such a relationship holds between all tokens and types in the classification S1 and S2, f connecting them is called infomorphism.

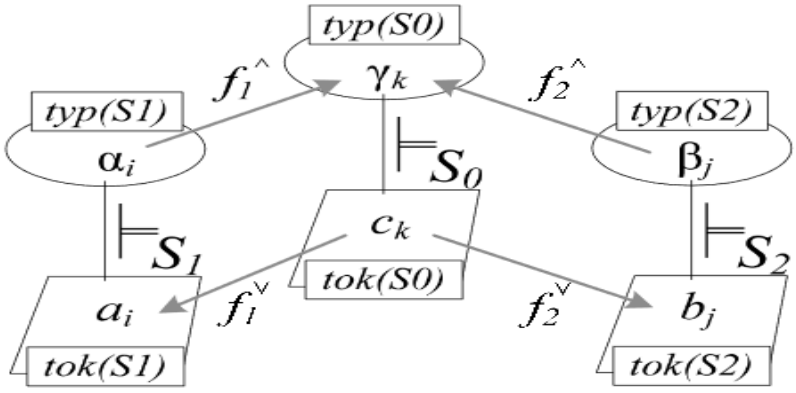

Fig.2 Channel

If there is a relation of information projection between three or more classification areas, it is shown in Fig.2. It is shown as, but at that time, the kind that has a relation of information with some other classification area like the classification area S0 is called the nucleus of the channel. Also, a group of information shoots that go to one core is called a channel.

For example, when considering one circuit A, the classification area A has a token A and a type A for classifying the tokens. Consider the bulb and the switch left and the switch right. The light bulb and the left / right switches are the elements that make up the circuit A, but the classification area: the light bulb and the classification area: the classification area A with the left / right switches. Each category has a type

depending on the token and component at some point in time (eg on / off).

To put this circuit to practical use, it is regularity that allows each switch to guess under what circumstances the bulb will turn on / off. This regularity determines the combination of tokens and types that each classification area has, called local logic. Regularity associates information that maintains regularity from one component to another. Such a set of components is called a channel, and there is a core of channels that form regularity and connect the components.

For example, suppose you want to turn on two switches to light a light bulb. When someone turned a switch on (a) the bulb turned on (I do not know what happened to the other), b) when a switch turned off the bulb did not turn on. There is no contradiction in each of these examples (but I don't know what happens to the other), but there is no consistency in when the light bulb turns on.

In the case of the circuit A, even if it is found that the bulb lights up when both the left / right switches are turned on at a certain point, the left / right I do not know what happens to the bulb when either is on and either is off. The Information flows through the core and flow regularity can create it.

The Local logic itself can be apparently created only by combinations of tokens and types, but in order for information to flow, it is necessary to satisfy such regularity. Anonymity is to allow the existence of a local logic that does not satisfy regularity. At this time, no information flows.

Now consider this situation as a consensus building protocol. Figure 3 is. The details of General Byzantine issues are as follows. In this situation, General 1 is the traitor, and General 3 is lost in judging which order is correct. Although the consensus building protocol in such cases has already been resolved, it goes without saying that the local logics of each general need to be consistent.

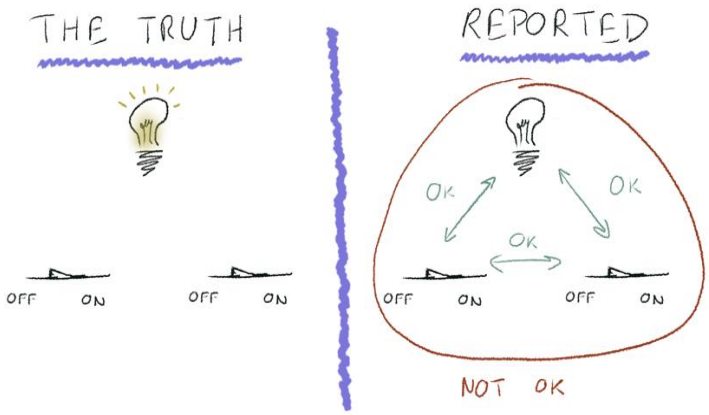

Fig3. Circuit

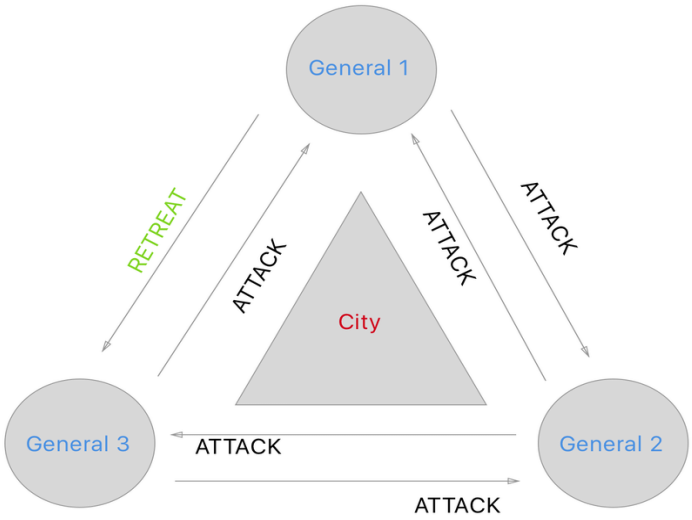

Fig4. General Byzantine problem