Research online Publishing
www.ronpub.com

Open Access

Open Journal of Web Technologies (OJWT)
Volume 5, Issue 1, 2018
http://www.ronpub.com/ojwt
ISSN 2199-188X

Anonymous Shopping in the Internet by Separation of Data

Sven Groppe [A], Felix Kuhr [A], Mehmet Atilla Coskun [B]

[A] Institute of Information Systems (IFIS), University of Lübeck, Ratzeburger Allee 160, 23562 Lübeck, Germany, {groppe, kuhr}@ifis.uni-luebeck.de
[B] Coolshae - Global Chain of Smallholders, 3 Kabaagac Ayvalik, 10400 Ayvalik, Balikesir, Turkey, atilla.coskun@bealdinproject.com

Abstract

Whenever clients shop in the Internet, they provide identifying data of themselves to parties like the webshop, shipper and payment system. These identifying data merged with their shopping history might be misused for targeted advertisement up to possible manipulations of the clients. The data also contains credit card or bank account numbers, which may be used for unauthorized money transactions by the involved parties or by criminals hacking the parties' computing infrastructure. In order to minimize these risks, we propose an approach for anonymous shopping by separation of data. We argue for the feasibility of our approach by discussing important operations like simple reclamation cases and criminal investigations.

Type of Paper and Keywords

Visionary paper: *trust, privacy, privacy-by-design, e-commerce, anonymous shopping*

1 Introduction

The percentage of end-consumers in the European Union ordering products or services via the Internet is continuously increasing from 23% in 2007 up to 48% in 2017[1]. This is only one of many survey results indicating the increasing impact of online shopping in daily live. Hence there is a need of analyzing the drawbacks of online shopping in order to overcome these by refined approaches to online shopping.

One main drawback of online shopping is that clients' shopping histories can be tracked and analyzed by the webshops for the purpose of market research, personalized and targeted marketing and other forms of clients' manipulations. Webshops may also sell their collected data about their clients to third-parties. It is known that even other parties in online-shopping sell their clients' data: For example, the bank ”Barclays” sells information on their clients' spending habits to other companies [10] and the shipper ”Deutsche Post” sold voter microtargeting data before the 2017 elections in Germany [5]. The discussion just started about how critical manipulations based on Big data analysis can be when looking at the Cambridge Analytica files reporting election manipulations based on Facebook data [19].

In order to avoid the misuse of data in the case of

This paper is accepted at the *International Workshop on Web Data Processing & Reasoning (WDPAR 2018)* in conjunction with the 41st German Conference on Artificial Intelligence (KI) in Berlin, Germany. The proceedings of WDPAR@KI 2018 are published in the Open Journal of Web Technologies (OJWT) as special issue.

[1] `https://de.statista.com/statistik/daten/studie/153980/umfrage/internetkaeufe-durch-einzelpersonen-in-der-eu-15-seit-2002/`

online shopping, the way of online shopping should be designed in a way to make data collection about the clients hard or even impossible. Clients should not only be pseudonymous (i.e. not linked to their real identity), but also protected in a way that the shopping history of one single client cannot be tracked and analyzed (avoiding the danger of clients becoming identifiable after some transactions) at any of the online shopping partners like webshop, bank and shipper. We call this way of online shopping *anonymous shopping* in the Internet.

Not only clients would benefit from a way to shop anonymously in the Internet. Among those end-consumers never shopping online, the key reasons they do not are a lack of trust (49%) and they have heard bad things about online shopping (25%) [4]. Hence if webshops offer a proven way to anonymous shopping, then clients would trust these webshops more than others without anonymous shopping feature resulting in more orders. Some webshops may weight client's trust in anonymous shopping more than the benefits of data analyis of client's shopping history. There might be also a point in the future after some more data scandals where politicians come to the glue that they need to actively protect citizens by paving the way for anonymous shopping. For not loosing the support of public authorities and the legislative authority, it is important that criminal investigations are still possible with a reasonable effort.

Main difficulties for staying anonymous during shopping in the Internet are the payment process and the shipping of goods. During the payment process any trace back to a credit card number or bank account means the loss of anonymity, while using the credit card or bank account is the most comfortable way to pay. For client's acceptance, we need an approach, which is not less comfortable than these most often used ways to pay in the Internet. Shipping to the home address is inherently non-anonymous, because clients have to provide their identities and addresses. However, we argue that not all involved partners need to know all or much data for the overall process, but we can separate the necessary data, such that the data retrieved by each partner is reduced to the absolute minimum.

The contributions of this paper are:

- an analysis of current possibilities to shop anonymously
  - in physical stores and
  - in the Internet.
- a proposal for anonymous shopping in the Internet
  - where each partner retrieves only those data that is minimal necessary for operating,
  - with a short analysis of the level of privacy,
  - a discussion about the practicability of the aproach,
  - the way to handle simple reclamation cases, and
  - means for criminal investigations.

2 Analysis of current Possibilities to Shop Anonymously

We describe the possibilities to shop in an anonymous way in physical stores in Section 2.1 and compare these possibilities with the most possible anonymous way for shopping in the Internet in Section 2.2.

2.1 Anonymous Shopping in Physical Stores

The simplest way of anonymous shopping is the traditional way: The client just goes to a (physical) store, pays by cash and takes him-/herself the products home. Client's shopping history is only tracked if

- the salesperson knows the client in person (or gets to know the client because of frequent client's store visits) and hence remembers the client's preferences. In this case the salesperson may also point to certain offers, which might be interesting especially for the client. Probably these kinds of interactions are the first forms of targeted and personalized advertisement.
- the client pays by credit card or bank card. This transaction identifies the client. In this way the client's shopping history can be even tracked.
- the client participates in loyalty programs. Clients pay benefits of loyalty programs like discounts with being tracked regarding their shopping history for marketing research and targeted advertisement purposes.

2.2 Anonymous Shopping in the Internet

The main difficulties to stay anonymous during shopping in the Internet are to stay anonymous during payment and stay anonymous for delivery purposes. In the following sections we describe operating services for both purposes.

2.2.1 Anonymous Payment

Gift Cards (at least of big players in eCommerce) can often be paid via cash and allow their users to buy products at a certain webshop up to the amount they hold. In this way their users stay anonymously during buying the gift cards and they cannot be identified when they use the gift cards for payment. However, the gift cards can only hold a certain amount of money. In order to detect cases of money laundering, retailers of gift cards have to report people buying large numbers of gift vouchers with cash, such that warnings are automatically triggered[2]. Hence gift cards are not suitable for anonymous payment of high-price products.

Prepaid Debit Cards have similar benefits for anonymous payment as gift cards, whenever prepaid debit cards are paid with cash, and are not reloaded after running out of money and hence are changed more often. This avoids comprehensive tracking of clients based on their credit card numbers. In comparison to gift cards, prepaid debit cards come sometimes with additional services like the ability to withdraw cash at ATMs. Unlike regular debit cards, prepaid debit cards would not provide access to the client's bank account if criminals hack the account or the debit card company. However, some prepaid debit cards cannot hold big values of money. Prepaid debit cards may also be not so comfortable to handle (because you need to reload or - for more privacy - change them more often).

Third-Party Services offer to mask their clients' purchases and identities by providing virtual phone, credit card and email address the clients can use instead of their own ones[3]. These services sit between the client and webshop, which charges the third-party service instead of the client directly, such that the client is neither traceable nor identifiable by the webshop. The third-party service afterwards charges the client. The main drawback of this approach is that the third-party service records the transactions of their clients. These recorded transaction may be misused by the third-party service itself or by criminals which may hack the third-party service.

Mobile Wallets of certain companies also hide their clients' identities to the webshop. For example, Apple Pay uses tokenization to keep the clients' identities and card numbers secret. The webshop receives only a device-specific token and a dynamic, one-time-use security code. The credit card number is determined by the payment network according to the token. Hence the webshop does not get to know the clients' identities, but the clients' banks and the used payment networks become aware of the details of the transactions. Google Pay offers similar possibilities, but Google Pay stores the clients' card numbers and the history of transactions on its own servers, which may raise concerns because of Google's advertising-focused business model.

Bitcoin uses peer-to-peer technology with no central authority (like a bank) involved to implement an electronic currency. Users are able to send and receive bitcoins without providing any personal identifying information, but each transaction is for everyone transparently stored in the Bitcoin's blockchain. Hence, according to [3] it is complicated to reach reasonable anonymity with Bitcoin, and perfect anonymity may be impossible. By enough analyzing capabilities this may even hold for bitcoin mixing services[4] that try to obfuscate bitcoin transactions by randomizing intermediate receivers, the amounts and delays of transactions.

2.2.2 Anonymous Delivery

P.O. Boxes: Regular **post-office boxes** are typically not meant to be used in an anonymous way. Indeed the address of a post-office box typically contains the private or company name of the recipient. Private Box in New Zealand [15] offers a mailbox that do not carry the client's home address, but still his/her name.

[18] reports on the company iPrivacy LLC, which operated in the late 1990s. iPrivacy offered to obfuscate clients' street addresses, which is only determined by the delivery company software after reaching the local postal area. As an alternative, iPrivacy allowed to pick up a parcel after anonymous verification from a local delivery depot.

Mail forwarding services: Snail mail [21] and Rapid Remailer [16] in the U.S. and Mail ghost [12] in the UK offer to forward parcels to clients' addresses after receiving them under another address and repackaging. These services may be also used to hide the original address of the sender. According to [17] Jimmy Carter used Snail mail to avoid the NSA surveillance programs.

The described approaches to anonymous delivery have the drawback that the shipper becomes aware of the link between client and webshop. In the next section we propose our approach to anonymous shopping and delivery without sacrificing comfort and providing a higher level of anonymity by introducing more partners in the overall system for the purpose of further separation of data.

[2] [13] reports a case where a woman tried to hide her pregnancy from online marketers. Her husband ran into difficulties when he tried to buy $500 of gift cards from Amazon.

[3] One such example of a third-party service is Blur from Abine, Inc., see `https://abine.com/index.html`

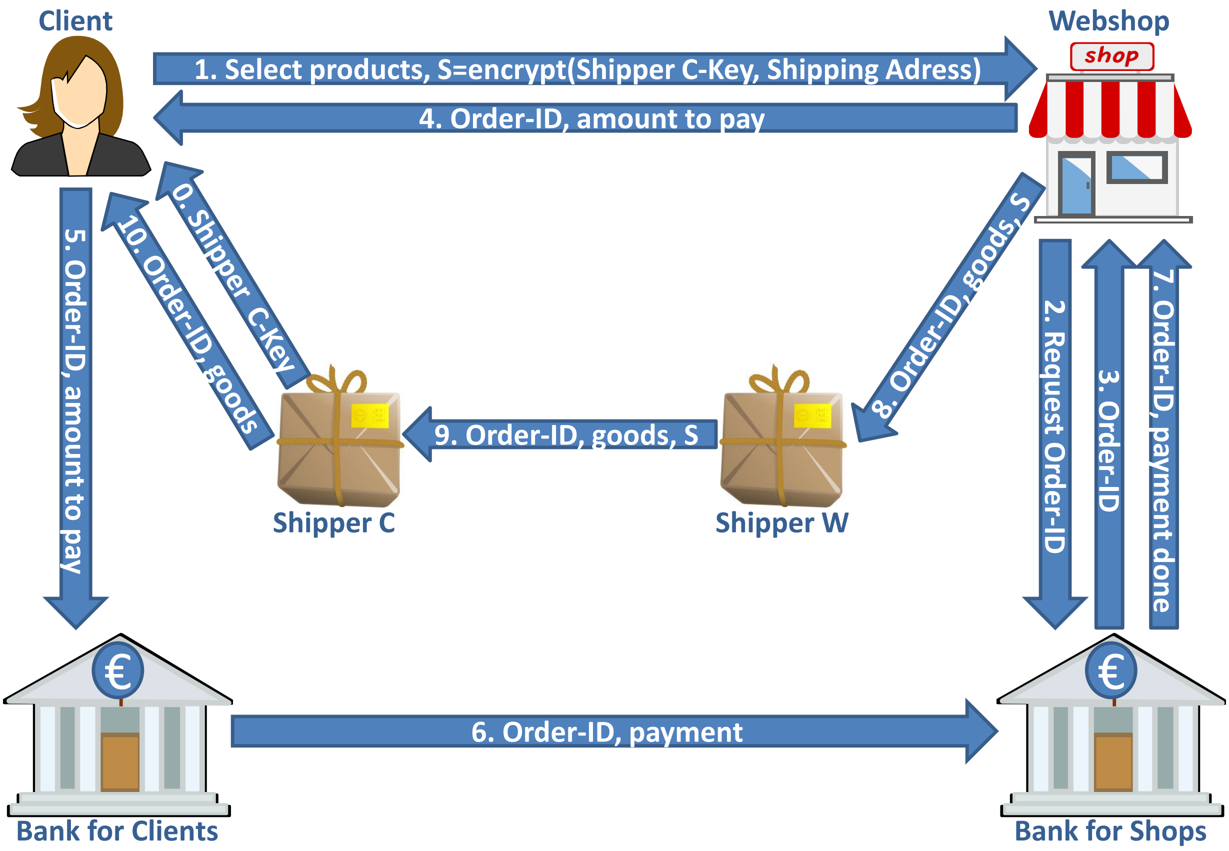

Figure 1: Overview of the approach to anonymous shopping in the Internet

3 AN APPROACH TO ANONYMOUS SHOPPING IN THE INTERNET

In our approach to anonymous shopping we introduce several partners for the purpose of separation of data:

- the client who wants to shop in an anonymous way,
- the webshop offering anonymous shopping,
- the bank for webshops operating the transactions with the webshop,
- the bank for clients operating the transactions with the clients,
- shipper W, which receives the parcels from the webshop, and
- shipper C, which delivers the parcels to the clients.

It must be ensured that all these partners are distinct companies that do not exchange any other data than those described in the following paragraphs. This may be achieved by a specialization of the bank for webshops to business customers and the bank for clients to end-customers. In a similar way the shippers W and C may be specialized shippers for webshops and end-customers.

Our approach to anonymous shopping consists of 11 steps of interactions between the involved partners (see Figure 1). Note that we only present the steps in a simplified form and do not describe security mechanisms for encrypted data exchange and authentication here. Please be aware of that standard mechanisms like SSL connections for encrypted message exchange and signatures for authentication purposes must be dealt with on top of the described steps. We also do not discuss methods here for avoiding the tracking of the user's IP address, MAC address, the computer's or browser's fingerprint [6] of the user, website's visits via cookies and similar track-able properties of the user's hardware devices or browser. For the purpose of non-tracking, the user should hence additionally apply already well-known techniques like disabling cookies and javascript (but many websites do not work without enabling javascript), and may use the browser Tor [14].

We describe each step in the following enumeration in more detail:

0. The client retrieves the public key of shipper C before (s)he goes for online shopping. The client may get the public key of shipper C from its database or from

[4] For example, see `https://coinmixer.se/de/`.

a public store of public keys.

1. Afterwards the client selects his/her products at a webshop offering anonymous shopping. The client encrypts his/her name and address with the public key of shipper C, such that only shipper C with its private key can decrypt these identifying information. The client transmits this encrypted information S along with the order.
2. The webshop calculates the amount to pay and requests an order-id at the bank for webshops.
3. The bank for webshops returns the newly created order-id, which serves as identifier for the order at all involved partners.
4. The webshop informs the client (within the same web-session) about the order-id and amount to pay.
5. The client instructs the bank for clients with the payment for the order with the given order-id.
6. The bank for clients transfers the money to the bank for webshops by annotating the transaction with the order-id (but *not* with any identifying information like bank account numbers of the client or the webshop).
7. The bank for webshops acknowledges the payment for order-id to the webshop.
8. The webshop packages the ordered goods, which are picked up by the shipper W. The shipper W also receives the order-id and the secret S.
9. The shipper W transfers the parcel with the ordered goods together with the order-id and secret S to shipper C.
10. Shipper C decrypts the secret S in order to receive the client's name and address and delivers finally the parcel to the client.

Due to simplicity of presentation the enumeration of the steps do not include communication for acknowledging the receipt of the previous message. For example, within step 5 the bank for clients additionally acknowledges to the client that it received the order-id and the amount to pay from the client. Of course the bank for clients should send the acknowledgment only after it writes the data to a log, such that the data is not lost in case of a crash and the whole process continues after recovery of the crashed components.

3.1 Short Privacy Analysis of the proposed Approach

The proposed approach to anonymous shopping is designed for privacy by strictly separating the necessary data. Table 1 lists which partner of the anonymous shopping system becomes aware of which data. Partners can only become aware of more data if they exchange their data. This must be guaranteed to not happen (except of cases of criminal investigations (see Section 3.4)). In the ideal case each partner supports independent agents, which control the data flow and check if no other data between the partners are exchanged than the designated ones. Of course no agent must be responsible for more than one partner in order avoid a leakage at the agents.

Only the client is aware of all data. The webshop only gets to know the ordered products and can calculate the amount to pay for the client. The webshop does neither know the identity of the client nor have a way to contact the client after the ordering process. By offering shopping without registration, the webshop cannot track clients' shopping history and preferences.

The client's bank cannot track a history of webshops with the amount to pay of ordered products. With our approach, the client's bank can only track and analyze the frequency of electronic orders with their amounts to pay.

The shop's bank does not get to know the client's identity. Hence the shop's bank can only track and analyze the frequency of orders of the webshop with their amounts to pay.

The shipper W gets to know that there is an order of products from the webshop, but without retrieving the client's name and address. Hence the shipper W can track and analyze the frequency (as well as maybe parcel volume) of orders at its serviced webshops, but cannot link these analysis results to clients. The shipper C only holds the data of the clients. Hence the shipper C may log and analyze the number and sizes of parcels the clients get, but the shipper C cannot link these information to webshops.

If in the design of our approach would be only one shipper, then this shipper would be able to track the links between webshops and clients decreasing clients' privacies.

3.2 Handling Simple Reclamation Cases

Simple reclamation cases without loosing the client's anonymity can be handled via order-id:

1. The client sends the product back to the webshop only stating the order-id (especially without giving his/her full address). The client may preferable use the same shipper C from which (s)he received the goods before, which forwards the parcel to shipper W. In this case the shipper C can look up his/her address by using the order-id in seldom cases when the parcel cannot be delivered by shipper W (and hence already returned to shipper C) for reasons like

    - the webshop ran into insolvency,

Table 1: Which partner in the proposed approach to anonymous shopping becomes aware of which data?

Partner	Data
client	webshop, ordered products, order-id, amount to pay, client's name and address
webshop	ordered products, order-id, amount to pay
bank for clients	client's name and address, order-id, amount to pay
bank for shops	webshop, order-id, amount to pay
shipper W	webshop, order-id
shipper C	client's name and address, order-id

- the webshop has moved to another location, or
- the webshop does not accept the parcel.

2. If the webshop accepts the reclamation, the money is transferred back from the bank for shops to the bank for clients annotating the transaction with the order-id.
3. The bank for clients finally transfers the money to the bank account of the client (by looking up its log of transactions with the annotated order-id).

In this way the participating organizations and companies (shipper C and shipper W, webshop, bank for shops, bank for clients) do not retrieve any other information than before (except that there is a reclamation case of a previous order having the given order-id). Hence even in simple reclamation cases client's anonymity is not lost.

The client's anonymity is only lost in complicated reclamation cases, where the webshop does not accept the reclamation. In this case the client may sue the webshop, which - by law - cannot be done in an anonymous way.

3.3 Practicability

We will discuss the practicability of our approach in this section.

The approach is designed to be similar comfortable for the client compared to non-anonymous shopping. The client might use a shopping-app developed for anonymous shopping in various webshops requiring a standardization of the APIs of the systems involved in the anonymous shopping process. This shopping-app can load (and verify) the public key of the shipper C during installation (without needing clients' interactions), which can be used afterwards for future shopping. Afterwards the shopping-app might provide a comfortable search for and selection of products in the webshops offering anonymous shopping. Of course it must be taken care that the shopping-app itself does not transfer any clients' data except of those necessary for anonymous shopping, but this might be ensured via certification of the shopping-app by *independent* control organizations. The costs for verification of the shopping-app might be taken over by the participating webshops or can be covered by selling the shopping-app. The payment process and providing the data for shipping purposes might be also integrated into the shopping-app in a comfortable way.

The payment process is not or not much more complicated in comparison to today's shopping experience, because today the billing process is often outsourced by the webshops to specialized companies, which also introduces another party. As in our approach the whole payment process can be handled by electronic means between the four partners webshop, client, bank for clients and bank for shops, the overhead costs are relatively low and - under the assumption of using networks with low latencies - might only take few milliseconds.

The transfer of the parcel from shipper W to shipper C might take some time. However, shipper W and shipper C might tune their schedules of receiving and delivering parcels in a way that no additional shipping day is needed. Furthermore, the costs for shipping might slightly be increased because two shipping companies are now involved instead of one. However, we expect the costs not to double because of optimizations of shipper W for mass delivery to few stations of shipper C.

3.4 Criminal Investigations

It might be necessary to investigate which clients ordered a certain product, because this product may be found at a location, where a criminal act has been taken place. For this purpose, the police may ask the partners to transfer their data to the police, where the data can be merged to analyze all data.

If the money transactions are not needed by the police, but only which clients ordered which products, then they may only ask for the webshop's and shipper C's data. If there is an investigation against the webshop (e.g. in cases of tax frauds), then - in order to retrieve the list of ordered products - the police needs the help of clients (or the police may order themselves products in some form of undercover investigation), but may need also the data of the involved banks.

Anyway there should be some obstacles for the police to retrieve the data from the partners of the anonymous shopping system, which may also hinder criminals imitating false identities of policemen. Hence the law may be reworked such that partners are only allowed to deliver data in case of court injuctions.

4 Related Work

The patents [7, 11] also use an order-id (or information to identify the order) as link for anonymous payment and delivery, such that anonymity of the client to the merchant is ensured. We propose to introduce more partners in the overall system in order to further separate the data for the purpose of increasing the anonymity. Hence in contrast to [7, 11], in our approach neither the banks nor the shippers do not know the link between merchant and client.

We describe the further related work to anonymous payment in Section 4.1 and anonymous delivery in Section 4.2.

4.1 Anonymous Payment

[22] proposes an anonymous payment system involving the three entities purchaser, merchant and issuer (the bank in the typical case) by using verification codes to keep the buyer anonymous. Their approach is designed for being used on a mobile payment platform with special focus on Wechat. In their approach and as first step, the buyer must deliver cash to the issuer, which is not so comfortable than just using a credit card or bank account for payment. In our proposed approach we designed an approach, which is comparable comfortable to the non-anonymous online shopping.

[1] describes an anonymous proximity mobile payment model with the goal of hiding customer's information from the merchant. In their approach, the authors also introduce two financial institutions (from the customer and the merchant) to increase anonymity in the payment process. However, they did not deal with simple reclamation cases (where the client still stays anonymous) and in their approach spent money may not be refunded in the case of dispute. [1] further specializes on mobile payment by relying on technologies like near-field-communication (NFC), whereas our contribution focuses on anonymous shopping in the Internet with anonymous delivery.

[8] introduces an anonymous and multi-vendor hash-based micropayment scheme. Again, the authors did neither deal with simple reclamation cases (ensuring client's anonymity) nor with anonymous delivery.

4.2 Anonymous Delivery

Inspired by Tor's onion routing approaches, [2] describes a blockchain based system called Lelantos for delivering goods, which offers client's anonymity and seller-buyer unlinkability. For the purpose of an almost impossible tracing, Lelantos utilizes blockchain pseudonymity and decentralization for providing pseudonymous delivery of goods. In comparison to Lelantos, our proposed anonymous delivery system offers a more comfortable delivery to the home address staying anonymous, which remains linkable when the partners merge their data (because of e.g. criminal investigations).

Some patented protocols like [20, 9] propose to utilize a proxy service for the purpose of hiding clients' identities from the merchants. In their approaches the shipper knows both the client and the merchant, whereas our approach provides a higher level of anonymity by using two different shippers, where one only knows the merchant and the other only the client.

5 Summary and Conclusions

In this paper we analyzed the today's possibilities to stay anonymous during the whole process of shopping in the Internet. After recognizing the limitations of today's possibilities of anonymous shopping, we propose an approach to anonymous shopping in the Internet, which is based on separation of data for raising the obstacles for intrusion into privacy by the involved partners or by criminals. We discuss the minimal necessary data of the involved partners required in the anonymous shopping process and the way how the partners can retrieve their necessary operational data. We further investigate simple reclamation cases and show that the clients stay anonymous also in these cases. We also argue that in cases of criminal investigations there is only a reasonable small overhead to retrieve the required data.

The proposed approach to anonymous shopping has the drawback that many partners are involved. Hence it will be difficult for small start-ups to convince so many other companies to become partners in an anonymous shopping system. Hence the system needs the support of big players picking up this idea or there is a strong political interest in (and funding of) such a system for anonymous shopping for protecting the clients' privacies.

References

[1] S. Almuairfi, P. Veeraraghavan, N. Chilamkurti, and D.-S. Park, "Anonymous proximity mobile payment (APMP)," *Peer-to-Peer Networking and Applications*, vol. 7, no. 4, pp. 620–627, 2014.

[2] R. AlTawy, M. ElSheikh, A. M. Youssef, and G. Gong, “Lelantos: A blockchain-based anonymous physical delivery system,” *IACR Cryptology ePrint Archive*, 2017, https://eprint.iacr.org/2017/465.pdf.

[3] Buy Bitcoin Worldwide, “Bitcoin anonymity - is bitcoin anonymous?” https://www.buybitcoinworldwide.com/anonymity/, accessed: 2018-04-18.

[4] Centre for International Governance Innovation, “2017 cigi-ipsos global survey on internet security and trust,” https://www.cigionline.org/internet-survey, 2017, accessed: 2018-04-18.

[5] J. Chase, “Deutsche post sold voter microtargeting data to CDU and FDP,” Deutsche Welle, http://p.dw.com/p/2vL6O, 2018, accessed: 2018-04-18.

[6] A. Gómez-Boix, P. Laperdrix, and B. Baudry, “Hiding in the crowd: An analysis of the effectiveness of browser fingerprinting at large scale,” in *Proceedings of the World Wide Web Conference*, 2018, pp. 309–318.

[7] T. Hataguchi, “Anonymous purchase and sale system for online shopping and delivery services via computer networks,” 2001, US Patent App. 09/826,244.

[8] A. Huszti, “Anonymous multi-vendor micropayment scheme based on bilinear maps,” *Proceedings of International Conference on Information Society (i-Society)*, pp. 25–30, 2014.

[9] R. C. Johnson, “edropship: methods and systems for anonymous ecommerce shipment,” 2010, US Patent 7,853,481.

[10] R. Jones, “Barclays to sell customer data,” https://www.theguardian.com/business/2013/jun/24/barclays-bank-sell-customer-data, 2013, accessed: 2018-04-18.

[11] K. Kobayashi, K. Takahashi, and H. Ohkoshi, “Anonymous electronic funds transfer system and method, and anonymous shipping system and method,” 2004, US Patent App. 10/733,342.

[12] Mail Ghost, “Anonymous mail forwarding,” http://mail-ghost.com/, 2018, accessed: 2018-04-18.

[13] J. Naughton, “Attempts to stay anonymous on the web will only put the NSA on your trail,” https://www.theguardian.com/world/2014/may/11/anonymous-web-nsa-trail-janet-vertesi, 2014, accessed: 2018-04-17.

[14] M. Perry, E. Clark, and S. Murdoch, “The design and implementation of the tor browser,” https://www.torproject.org/projects/torbrowser/design/, 2013, the Tor Project.

[15] Private Box, “Manage your po box online, mail forwarding forwarding, scanning and virtual office services,” https://www.privatebox.co.nz/, 2018, accessed: 2018-04-18.

[16] Rapid Remailer, “Anonymous letter and package remailing service,” http://rapidremailer.com/, 2018, accessed: 2018-04-18.

[17] Reuters, “Jimmy carter sticks to ’snail mail’ in missives to world leaders,” https://www.reuters.com/article/us-usa-security-carter/jimmy-carter-sticks-to-snail-mail-in-missives-to-world-leaders-idUSBREA2M0QI20140323, 2014, accessed: 2018-04-18.

[18] B. Rosenberg, *Handbook of Financial Cryptography and Security*, 1st ed. Chapman & Hall/CRC, 2010.

[19] S. Siddiqui, “Cambridge analytica’s us election work may violate law, legal complaint argues,” https://www.theguardian.com/uk-news/2018/mar/26/cambridge-analytica-trump-campaign-us-election-laws, 2018, accessed: 2018-04-18.

[20] S. Stolfo, J. Smith, and J. Chung, “Method and system for private shipping to anonymous users of a computer network,” 2001, US Patent App. 09/754,897.

[21] Ultimate Privacy, “Anonymous snail mail - real world anonymity,” http://www.ultimate-anonymity.com/snail-mail.htm, 2018, accessed: 2018-04-18.

[22] J. Wu, C. Liu, and D. Gardner, “A study of anonymous purchasing based on mobile payment system,” *Procedia Computer Science*, vol. 83, pp. 685 – 689, 2016.

AUTHOR BIOGRAPHIES

Sven Groppe earned his diploma degree in Informatik (Computer Science) in 2002 and his Doctor degree in 2005 from the University of Paderborn. He earned his habilitation degree in 2011 from the University of Lübeck. He worked in the European projects B2B-ECOM, MEMPHIS, ASG and TripCom. He was a member of the DAWG W3C Working Group, which developed SPARQL. He was the project leader of the DFG project LUPOSDATE, an open-source Semantic Web database, and one of the project leaders of two research projects, which research on FPGA acceleration of relational and Semantic Web databases. He is also the chair of the Semantic Big Data workshop series, which is affiliated with the ACM SIGMOD conference (so far 2016 to 2018), and of the Very Large Internet of Things workshop in conjunction with the VLDB conference in 2017 and 2018. His research interests include databases, Semantic Web, query and rule processing and optimization, Cloud Computing, peer-to-peer (P2P) networks, Internet of Things, data visualization and visual query languages.

Felix Kuhr earned his M.Sc. in Informatics in 2015 from the Technical University of Hamburg. Felix worked as a master's student in the PANOPTESEC integrated research project (FP7 of the European Commission) for the University of Lübeck. Currently, he is a PHD student at the University of Lübeck and co-founder of a data network company. His research interests include machine learning, data mining, data networks and security.

Mehmet Atilla Coskun studied Marine Engineering in Technical University of Istanbul but he worked in other fields such as in advertising as Copy-writer, in sales and marketing as manager, in e-business as project consultant and developer. Coshun was also prize winner song writer and author of a bunch of fictional books. He worked in the multidisciplinary Bealdin Project in the role of bridging different disciplines together and providing project vision.