Abolition of cash – the end of data privacy

Von Christoph Winnefeld und Stephanie Dold

Die Verschiebung des Bezahlverhaltens zu immer mehr bargeldlosen Zahlungen mag bequem sein – sie birgt allerdings auch Datenschutzrisiken. Debit- und Kreditkarten nehmen die Autoren hier nicht aus. Im Vergleich verschiedener Verfahren sehen sie die größten Risiken bei Amazon Go, wo Rechtsverstößen zumindest kein Riegel vorgeschoben ist. Bei Wechat Pay liest die chinesische Regierung mit und bei Alipay ist das Sammeln von Daten das Geschäftsodell. Am sichersten sind Daten der Analyse zufolge bei Apple Pay. Die Schlussfolgerung der beiden Autoren: Eine Bargeldabschaffung hätte fatale Folgen für den Datenschutz im Payment. Red.

Even though cash has been of huge significance for several centuries, it is increasingly being replaced by new alternatives. When looking at online shopping in Germany in 2019, it is noticeable that goods and services were mostly paid with online payment methods like Paypal and Amazon Payments. With a 77 percent-share, online payment is even used more often than paying by invoice and by credit and debit card.

Privacy Protection versus Abuse of Privacy of Data

When registering for an alternative payment method, personal details must be provided. Without information such as inter alia name, bank number, date of birth, and email address, it is not possible to use the desired payment method. The protection of privacy is therefore very important when so many personal details have to be given to another party.

When paying with a credit card as well as a debit card, the whole payment process is not as anonymous as it would be with cash. First of all, when paying with a card, data is released. This means for example the bank code and the account number are getting visible for the retailer when making a payment. This is a factor that can ultimately lead to privacy abuse. When something is bought in a supermarket, the supermarket can classify the customer based on this released data and in the worst case, this can be misused for purposes the customers would never have thought of. This usually happens in conjunction with a customer card, as it contains exact personal information such as address, date of birth, email, etc. This means a lot of privacy is lost.

NFC involves risks

Furthermore, all payments made with the card are visible to both the cardholder and the bank. Thus, the bank afterwards can look at every single detail of a payment. This is the amount which was paid but also the location as well as the store and time. This insight therefore does not allow much privacy anymore. Additionally, most credit and debit cards have built-in chips that run with Near Field Communication (NFC), allowing contactless payment. Depending on the bank, a payment with an amount up to 50 Euros can be made without entering a PIN. This is very practical on the one hand, but also involves risks on the other hand.

NFC has the problem that without consciously paying, data can get to a third party. The data transfer is even possible if the card is inside a hand or shopping bag or a wallet. Thieves can easily catch data and thus have access to secret bank data of the targeted person. Meanwhile, many credit and debit cards work with NFC. They are constant

Dr. Christoph Winnefeld,
Dozent für Finanzwirtschaft
und Bankbetriebslehre,
Hochschule Trier

in transmission mode, which means that money is at risk to be stolen anytime.

Paypal without data privacy

Paypal is one of the most used online payment methods worldwide. By the end of 2019, Paypal counted 305 million users. In Germany, Paypal is considered the most used online payment method and also the most offered online payment method even before Mastercard. The use of Paypal is comparatively easy and fast. During the registration process only the bank account or credit card details have to be provided. Afterwards, just the email address and the corresponding password are needed to login and make a payment, which is processed in real time. Money can also be transferred between two people (C2C).

However, the amount of personal data which is released is often not considered. One has to be aware that data including the name of the person, the user's bank account information, the currency and the date of the purchase will be passed on to third parties. With the agreement of the general terms and conditions, it is therefore accepted that data can be passed on to the banking partners of Paypal and debt collection companies and in connection with shipping and similar services. Therefore, privacy is not safe when paying with Paypal.

Apple Pay with data encryption

Apple Pay is a payment system that runs on the newer generations of Apple devices like iPhones and Apple Watches. The payment with Apple Pay is quick and easy. A quick double-click on the power button is all it takes to unlock the mobile device, which then has to be held close to the payment terminal to proceed with the payment. Many German banks have meanwhile enabled Apple Pay, which can be used wherever contactless payment is possible.

When paying, no data is released to the retailer. The payment transaction is carried out via the device account number and a variable code. Therefore, the retailer has no personal details that could be used for personalised advertising or sales analyses. Apple with its payment solution Apple Pay does not store credit card numbers. Apple also does not keep personal data and information about the individual transactions and neither it gives data to the retailers. All personal data when making a payment through Apple Pay is encrypted for third parties.

The only data that Apple has access to is the location of the payments. Just like paying with a credit or debit card, the bank however knows about some aspects of the transaction, for example the paid amount, the time and the place of the transaction. In addition, when installing Apple Pay, the bank receives personal data like the device ID including the model number, location, telephone number for security checks, as well as the customer name and the corresponding billing address. The bank also receives information on whether purchases have already been made with the registered mobile phone at earlier times. In terms of privacy, Apple Pay guarantees its customers no personalised advertising based on purchases.

Less data protection with Google Pay

Google Pay works similar to Apple Pay. Google Pay can be used with the newer generations of smartphones that are operated with Android. However, not many German banks make it possible to use Google Pay so far.

In comparison to Apple Pay, data protection is less given with Google Pay. In the privacy policy of Google Pay, it is expressly stated that data can be collected with each transaction. When performing a transaction with Google Pay, the date and time of the purchase, the place and the merchant as well as the description of the goods are visible for Google Pay. With this information it is possible to play personalized advertising on the smartphone of the respective user. As all transactions are monitored this means a massive intrusion into the personal privacy. Only if the amount to be paid is higher than 25 Euros, the phone has to be unlocked. That means if a phone working with Android is stolen, it is possible that a thief can make several small payments. This is not possible with Apple Pay, where the device has to be unlocked for every single transaction.

Wepay is not anonymous

One of the most popular payment methods in China is Wepay. The app combined with a messenger function offers the possibility to pay easily and quickly and makes sending money very fast and simple. Payment is either linked to a bankcard or the money can directly be recharged to the Wepay Wallet account. When opening the app, a QR-code (for security reasons only valid for 60 seconds) appears, which has to be scanned by the seller or by the buyer. Both ways a payment can be processed. Only the paid amount needs to be typed in and the whole payment is completed.

However, data protection has to be considered critically. Payments are by no means anonymous when they are made with Wepay. The Chinese government insists that all data is stored for at least six months.

The rating app Sesame Credit, which is being tested in some cities in China at the moment, monitors the activities of every single citizen. Since social media, messaging services and payment are inter-linked, the social rating system makes it easy to monitor the activities of the customers.

Through the Sesame Credit app, citizens are rated and credit points can either be awarded or deducted. The rating app recognizes the products of a shopping cart and evaluates them. Chinese citizen with a high Sesame Credit rating can for instance obtain a passport faster than someone with a lower rating. A higher rating at Sesame Credit means being privileged when booking a hotel or getting better rank-

Stephanie Dold,
Hochschule Trier

ings in dating apps. Also, with a high rating it is possible to get a better job. On the contrary, a penalty for a low score could be, for example, a slow internet connection. Additionally, if the rating app realizes that a person is in close contact with someone who is very low ranked, it can result in that person getting lower rating points as well.

Thus, a payment with Wepay is not anonymous and not only the merchant and the bank can have insight into the payment but also the Chinese government.

Alipay ist mainly interested in data

Alipay is also mainly used in China, and competes with the aforementioned Wepay. Payments are executed simply and quickly with a QR code generated either by the seller or the buyer.

Data "protection" at Alipay is similar to Wepay. Alipay is mainly interested in the data of the customers, which are stored and regularly passed on to third parties. Alipay also delivers data to the Chinese rating system Sesame Credit. By the end of 2020 this system should be obligatory for all inhabitants in the area of Beijing. This way the behaviour of the population is monitored and consequently controlled. There is no privacy anymore when it comes to a payment. According to president Xi Jinping, the social rating system is intended to provide security for the population of China. He does not see the ranking system as an interference in privacy.

Amazon Go – a big caveat

At the beginning of 2018, a new payment system was created by Amazon. It is designed as a "just walk out" experience. A technology called Sensor Fusion makes it possible to leave the store without any physical payment at the end of the shopping, and without making people queue at the cashier desk. When entering an Amazon shop, a QR-code has to be scanned with the help of the app Amazon Go. Cameras and the use of deep learning computer algorithm automatically recognize which products are taken. All products are equipped with a RFID-chip (radio frequency identification). At the end of the shopping, the invoice is sent to the app. If this system proves its effectiveness, it could be that no cash or self-payment stations are needed anymore.

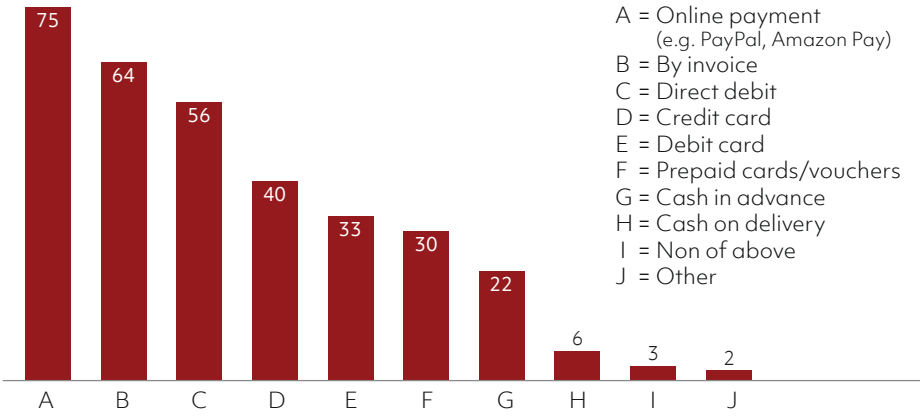
However, there is a big caveat in terms of data protection. Cameras scan people and products continuously so that the accuracy of the shopping cart can be assured. Machine learning makes it possible for cameras to remember customers and register their habits.

Critics emphasise that this way of surveillance breaches data protection laws. It is very likely that data captured by the cameras will remain stored on the server and thus profiles of individual customers will be generated. The complete monitoring of the stored data could as well potentially lead to price manipulation (for instance, beer prices suddenly rise before major sporting events, ice cream prices rise at the same time of a heat wave).

Another point regarding the misuse of personal data is that (theoretically) biometric data can be collected, which Amazon officially denies. However, through artificial intelligence, the implemented algorithm is able to identify body size, gait type or physical limitations such as wheelchair users.

In addition, stored data, such as customers' standard purchases or favourite products, would make it possible to produce personalised advertising in the shop for the personalised shopping basket and for similar or complementary products.

Online payment by type in Germany 2019



Share of respondents in percent

Source: Kunst, A. 2019. Statista

Smile-to-pay-payments use the "face print"

The Chinese are already a long way ahead of the Europeans when it comes to new methods of payment. New technologies make it possible to pay by face recognition: with just a smile a payment can be validated. The method to pay with a smile is possible because it is a universal human expression. The point-of-sale machines are equipped with 3D cameras which are able to recognize persons at the end of the shopping process just because of their faces and smiles. The recognition process is based on biometric data where approx. 600 points of each person´s face are scanned and saved.

This way, every person gets his or her own "face print". The more points are measured, the more reliable is the correct assignment to the corresponding person. A code is assigned to each face, which is then used for billing when the payment is made. For security reasons, the algorithm recognizes only living beings, so no payment can be made with a photo. In more than one hundred cities in China this technology is already used, for example in 7-eleven convenient stores or in the fast food chain KFC. As a result, payment is possible without any mobile phone, watch, card or cash.

Chinese do not seem worried about their privacy with this technology. They are more worried about not looking

good on the picture which is taken when paying with a smile. Alibaba already offers a solution for this "problem" and has developed a filter which lets people look friendlier on pictures.

Only cash can't be tracked

There are possibilities to take precautionary measures to prevent the risk of data being passed on to third parties. Mobile payment and contactless payment with NFC technology can easily be protected against data misuse by third parties. For credit or debit cards, there is the option of inserting a protection card in the purse or wallet which stops the transmission of NFC waves. The same applies to mobile payment, where it is possible to deactivate NFC, but this results into being not able to do contactless paying until NFC is activated through the bank again.

Another possibility to prevent the unnoticed debiting of cards is having several NFC-compatible cards in one´s purse or wallet. The NFC signal is disturbed if there are several cards near each other. Therefore, they only work if they are available individually or if they are taken out of the wallet or purse for payment.

Protection for the NFC technology for smartphones only comes with the Android phones, where it is possible to turn of settings for NFC. This option is not available for iPhones. Another way of protection for smartphones are mobile phone covers which have a built-in NFC blocker. This makes sure that no payment can be made and no one can steal data from it with a special device.

A further precautionary measure in the protection of privacy is the avoidance of public Wi-Fi networks when making online payments and mobile payments. Open and unsecured Wi-Fi networks allow criminals to access personal and payment data such as card number, CVV number, expiry date of the card, etc.

A possible abolition of cash could have fatal consequences for privacy. Cash is the only means of payment that guarantees full privacy and data protection. For all other methods of payment which have been described above, personal information is released when a transaction is made, no matter if a debit or credit card, an app, or even just a smile is used to make a payment. That means that with all these methods, payment can be tracked by the bank and/or personal data is released to third parties, possibly including the state government.

With the abolition of cash, any right of anonymous activities with regard to payments would be abolished. No other method of payment can come as close to the concept of the privacy as cash does. ■